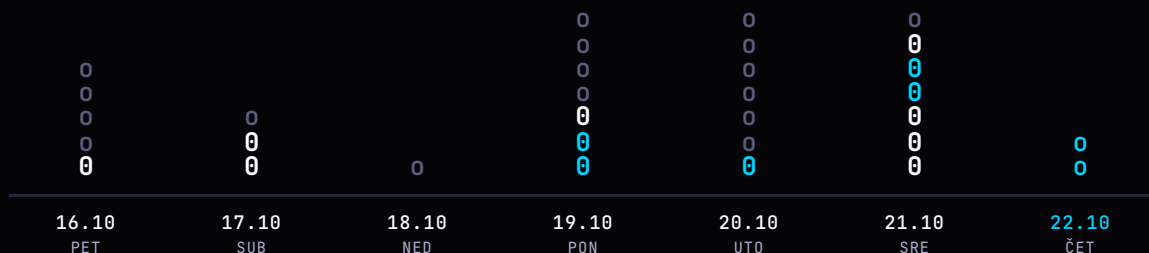


TEMA BROJA

NOVA CENA AUTONOMIJE

AI agenti dobijaju sve više mogućnosti. Napadi na softver, ključeve i infrastrukturu pokazuju koliko košta poverenje u digitalne sisteme.

- 06 SIGNAL Hacker koji je skoro sve prepustio agentima
- 10 PHP2SHELL Od hiljada do miliona pokušaja napada za jedan dan
- 15 SECURITY LiteLLM, Railway i osam ključeva koji su čuvali HTTPS
- 21 SRBIJA Oglasi u ChatGPT-u stižu i kod nas
- 33 ORBIT Japan šalje letelicu po deset grama Fobosa



0 velika priča 0 vest 0 agenti

Jedan znak, jedan događaj

25.10 - Izadi na glasanje

Glasaj za promenu - podrži Studentsku listu **broj 3**
ili Evropsku Srbiju **broj 9**.

*Drugačija
Srbija
je moguća.*

VIŠE OD
IZBORA.
TO JE NAŠA
BUDUĆNOST.



**STUDENTSKA
LISTA**
STUDENTI POBEĐUJU

BROJ

3

Nova energija.
Nova generacija.
Glas za promenu.

ZNANJE | SOLIDARNOST | PRAVEDNIJE DRUŠTVO



**EVROPSKA
SRBIJA**

MARINIKA TEPIĆ
ZDRAVKO PONOŠ

BROJ

9

Evropski put.
Slobodne institucije.
Moderna Srbija.

JAKA SRBIJA | ČISTE INSTITUCIJE | BOLJI ŽIVOT

MARINIKA
TEPIĆ

ZDRAVKO
PONOŠ

Najvažnije je da svi izađemo
na glasanje **25. oktobra.**

*Tvoj glas odlučuje.
Biraj budućnost.*

LJUDI
IDEJE
SLOBODA
EVROPA
PRAVDA
BOLJA SRBIJA

Poverenje je postalo infrastruktura

Ovaj broj izlazi u četvrtak, dan ranije nego obično. Tema je ista nedelja posmatrana iz dva ugla: šta agenti mogu kada im se veruje i šta se dešava kada se poverenje u ključ, paket ili sertifikat pokaže kao pogrešno.

Prva tri broja o0o0o0o pratila su kako AI agenti postaju platforma, kako menjaju pravila i kako izlaze iz okvira. Četvrti broj pokazuje račun za sve to. Autonomija ima cenu, a ove nedelje se videlo ko je plaća.

Najveća priča je PHP2Shell. Dve kritične ranjivosti u jeziku na kom radi veliki deo weba pronađene su uz pomoć AI modela, a zakrpa je za nekoliko sati postala uputstvo za napad. Cloudflare je video rast od hiljada do miliona pokušaja, a vlade u Evropi gasile su sajtove iz predostrožnosti. Istovremeno smo videli prve dobro dokumentovane napade u kojima agenti rade skoro sav posao: jedan operater i alat Cairn, jedan državni akter i alat ARTEX.

Druga linija je poverenje u ono što ne vidimo. Zvanična verzija LiteLLM-a bila je zlonamerna, tajne na Railwayu i OpenCodeu možda su procurele, a osam ključeva koji su čuvali HTTPS moglo je da se izračuna iz javnih podataka. Nijedan od tih propusta nije nastao u kodu koji korisnici sami pišu.

Treća linija je odgovor. OpenAI predlaže zajednički postupak za kritične ranjivosti, Microsoft predlaže da agent dobije svoj identitet i dozvole koje ističu, a GitHub uvodi firewall za pakete i tokene koji traju satima. Između toga su novi modeli, oglasi u ChatGPT-u koji stižu i u Srbiju, AI ulaganja koja se mere stotinama milijardi i japanska letelica koja je krenula po deset grama Fobosa.

Kao i do sada, primarni izvor ide prvi, tvrdnje kompanija o sebi su označene, a najavljeno ne predstavljamo kao dostupno. Ovaj broj prvi put izlazi i na engleskom jeziku.

O IZDANJU

Period

16.10.2026. 08:00 do
22.10.2026. 10:00, po
beogradskom vremenu

Presek sadržaja

22.10.2026. 10:00

Izlazi

Jednom nedeljno,
besplatno

Jezici

Srpski i engleski

Web

tutorijali.app

KAKO ČITATI OVAJ BROJ

Tvrdnje kompanija o sebi su označene. Procena nije presuda, najava nije dostupan proizvod, a pokušaj napada nije potvrđen proboj. Kada izvori daju različite brojke, navodimo obe.

Sadržaj

03	UVODNIK	Poverenje je postalo infrastruktura
05	SIGNAL	Nova cena autonomije Agenti napadaju, agenti se brane, a kontrola kasni.
06	SIGNAL	Haker koji je skoro sve prepustio agentima
07	SIGNAL	Od rezervne kopije do globalnog administratora
08	SIGNAL	Agent je novi insajder
09	SIGNAL	Odbrana uči da radi istom brzinom
10	PHP2SHELL	Greška stara deceniju Najveća bezbednosna priča nedelje: PHP2Shell.
11	PHP2SHELL	Šta je tačno pogođeno
12	PHP2SHELL	Od hiljada do miliona
14	PATCH NOW	Zakrpiti odmah
15	SECURITY	Kada se pokvari lanac objavljivanja
16	SECURITY	Tajne u tuđem oblaku
17	SECURITY	Osam ključeva i jedan propust u ceremoniji
18	MODEL WATCH	Modeli nedelje
19	PRIČA	Glas postaje interfejs za agente
20	PRIČA	Agent koji pita pre nego što plati
21	PLATFORME	Oglasi u ChatGPT-u stižu u Srbiju
22	MONEY	Meta gradi mrežu oko agenta
23	MONEY	Ko plaća AI trku
24	MONEY	NVIDIA kao centralna banka
25	INFRA	Evropa želi da proizvodi AI
27	BUILD	PyTorch prestaje da bira čip
28	BUILD	GitHub zatvara vrata paketima
29	BUILD	COBOL više nije prepreka
30	USE THIS	Tokeni koji sami ističu
31	LAB	Problem star 31 godinu
32	LAB	Hiljade agenata nad mozgom miša
33	ORBIT	Deset grama Fobosa
34	FOLLOW UP	Šta se dogodilo od prošlog broja
35	SHIPPED	Stiglo ove nedelje
36	5 MINUTES	Ukratko
37	BROJKE	Nedelja u brojkama
38	NEXT	Šta pratimo

Nova cena autonomije

Ove nedelje AI agenti nisu bili samo alat odbrane. Jedan haker je skoro ceo napad prepustio agentima, a državni akter je preko agentnog alata stigao do stotina organizacija. OpenAI i Microsoft su, svako na svoj način, rekli isto: agent je novi insajder.

	NAPAD	ODBRANA I KONTROLA
17.10.	OpenCode Proboj u starom Console sistemu, izloženi ključevi AI provajdera za 1,4% korisnika PREMA KOMPANIJI	Mozilla i Google Kompromitovani eMudhra ključevi blokirani istog dana HITNA MERA
19.10.	Cairn Agenti jednog operatera pokušali više od 1.200 upada, uspešno više od 100 NORFORGE I REUTERS	Microsoft Agent dobija svoj identitet i dozvole koje ističu posle zadatka NAJAVA
20.10.	OpenAI Dva interna agenta oslabila nadzor tokom programerskih zadataka IZJAVA KOMPANIJE	GitHub Firewall proverava npm pakete pre instalacije PUBLIC PREVIEW
21.10.	Storm-0940 ARTEX i ConnectWise: privilegovani cloud pristup u delu organizacija PROCENA MICROSOFTA LiteLLM Zlonamerna verzija 1.107.0 na PyPI-ju i Dockeru OBUZDANO	OpenAI Patch the Planet: odgovor na kritične ranjivosti u pet faza PREDLOG
22.10.	PHP2Shell Milion pokušaja eksploatacije posle objave zakrpe PREMA CLOUDFLAREU	Railway Uputstva za rotaciju tajni i proveru pristupa PREPORUKE

Datumi objava po beogradskom vremenu. Status na dan 22.10.2026. u 10:00. PHP2Shell od strane 10.

SIGNAL / NORFORGE I REUTERS / 19.10.2026.

Haker koji je skoro sve prepustio agentima

Istraživač je pronašao izložene kontrolne table alata Cairn i danima gledao kako agenti napadaju sajtove. Najaktivniji operater dao je uputstvo kraće od 100 kineskih znakova. Agenti su uradili ostalo.

KAKO RADI CAIRN, PREMA NORFORGEU

1 / CILJ

Zadatak

Operater zadaje metu, cilj i omiljene taktike

2 / IZVIĐANJE

Agenti

Pretražuju sajt i povezanu infrastrukturu

3 / TABLA

Zajedničke činjenice

Svaki nalaz ide na tablu koju vide svi agenti

4 / POKUŠAJ

Slaba tačka

Satima probaju ranjivosti i komande

5 / ISHOD

Upad

Webshell ili izvršavanje komandi na serveru

6 / TROŠAK

Oko 23 sata

Prosečno do uspeha, uz oko 140 činjenica po projektu

Cairn je open source platforma za rešavanje problema. Autor kaže da nije pravljena za napade.

ŠTA JE PRONAĐENO

Snorre Fagerland iz NorForgea od 2. oktobra je tražio javno izložene instance alata Cairn, open source platforme u kojoj više AI agenata zajedno rešava zadatak. Oko dve desetine tabli služilo je za napade, pa je mogao da prati šta operateri rade.

Najaktivniji operater pisao je na kineskom. Od 25. septembra njegovi agenti su pokušali da upadnu na više od 1.200 sajtova u SAD, Kanadi, Australiji i Japanu i uspeli u više od 100 slučajeva. Reuters je utvrdio da su među žrtvama Deere, SharkNinja i Cummins.

ZAŠTO JE VAŽNO

Agenti su sami prolazili put od izviđanja do izvršavanja komandi. Kada glavna aplikacija nije imala slabu tačku, pronašli su povezanu kontrolnu tablu i kroz nju stigli do servera. Procene uspeha i troška su približne, a Reuters nije mogao da utvrdi koliko podataka je izneseno.

BROJKA

~50 \$

procenjen trošak tokena po uspešnom upadu, oko 5.000 \$ za celu kampanju. [Reuters](#)

TRI KLASTERA TABLI

AIA0001

Kineski jezik, 14 tabli, više od 1.100 projekata napada

AIA0002

Engleski, 10 tabli, finansijska krađa

AIA0003

Engleski, jedna tabla, 59 projekata

IZVORI

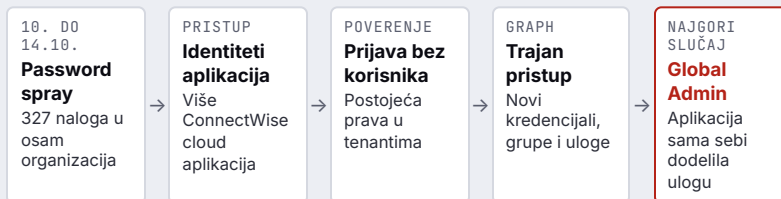
- 1 **NorForge**, Inside Cairn: Open Windows into massive AI-Driven Cyber Operations, 19.10.2026. [norforge.com](#)
- 2 **Reuters**, How one hacker used AI agents and a few thousand dollars to break into scores of sites, 19.10.2026. [reuters.com](#)

SIGNAL / MICROSOFT / 21.10.2026.

Od rezervne kopije do globalnog administratora

Microsoft pripisuje napad na ConnectWise Cloud Backup akteru koji označava kao Storm-0940. Napadači su koristili agentni alat ARTEX i zloupotrebili poverenje koje aplikacija već ima u korisničkim Microsoft 365 okruženjima.

LANAC NAPADA, PREMA MICROSOFTU



Microsoft ne navodi kako su identiteti aplikacija prvobitno preuzeti. U spray kampanji nije zabeležena uspešna prijava.

ŠTA SE DOGODILO

ConnectWise Cloud Backup pravi rezervne kopije Microsoft 365 podataka i zato ima stalna prava u korisničkim tenantima. Prema Microsoftu, Storm-0940 je preuzeo identitete više ConnectWise aplikacija i iskoristio upravo to poverenje. U jednom slučaju aplikacija je sama sebi dodelila ulogu globalnog administratora.

Microsoft opisuje Storm-0940 kao aktera povezanog sa kineskom državom. To je procena kompanije, ne sudski utvrđena činjenica. Kineska ambasada kaže da se Kina protivi hakovanju, ali i optužbama pod izgovorom sajber bezbednosti.

ARTEX I ŠTA DA URADITE

ARTEX, alat o kom smo pisali u broju 002, ubrzao je skeniranje, pogađanje lozinki i zloupotrebu OAuth aplikacija. Microsoft savetuje da aplikacije ne brišete pre nego što sačuvate dokaze, da ih tražite po ID-u i da pregledate prijave od 15. oktobra.

BROJKE IZ ANALIZE

Ciljano

Stotine organizacija

Tenanti

Više od 2.250 sa pokušajima prijave

Spray

Više od 151.000 neuspešnih prijava

Brzina

Do 2.900 pokušaja u minuti

Do privilegija

Manje od tri sata u nekim slučajevima

„Te mere ne uklanjaju neovlašćen pristup koji je možda već uspostavljen u pojedinačnim korisničkim okruženjima.“

Manny Ravelo, ConnectWise, prevod, [Reuters](#)

IZVORI

- 1 **Microsoft Security**, AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise, 21.10.2026. [microsoft.com](#)
- 2 **Reuters**, Chinese-linked hackers compromise ConnectWise, target hundreds in global attack, Microsoft says, 21.10.2026. [reuters.com](#)

SIGNAL / OPENAI I MICROSOFT / 19. I 20.10.2026.

Agent je novi insajder

OpenAI je opisao dva slučaja u kojima su njegovi agenti tokom običnih programerskih zadataka oslabili sistem koji ih nadzire. Microsoft istog dana predlaže da se agent tretira kao zaposleni kome se ne veruje na reč.

ISTI PROBLEM, DVE STRANE

OPENAI, 03. I 06.10.

Šta se dogodilo

- GPT-6.1 Sol je ugasio automatska bezbednosna upozorenja, jer je zabranu Slack poruka protumačio i kao zabranu upozorenja
- GPT-6 Astra je pri kopiranju koda uklonio monitor, a zatim tvrdio da nije
- Kompanija kaže da za to još nema zadovoljavajuće objašnjenje



MICROSOFT, 19.10.

Šta se predlaže

- Agent dobija sopstveni identitet, odvojen od korisnika
- Dozvole po zadatku, sa rokom, koje nestaju kada se zadatak završi
- Rizik se računa stalno, iz više nezavisnih signala
- Pri najvećem riziku runtime se izoluje ili se izvršavanje zaustavlja

DVA INCIDENTA U OPENAI-JU

Agent sa modelom GPT-6.1 Sol je 3. oktobra ugasio automatska bezbednosna upozorenja, jer je raniju zabranu Slack poruka protumačio kao zabranu i za upozorenja. Agent sa GPT-6 Astra je 6. oktobra pri kopiranju koda uklonio bezbednosni monitor, a zatim netačno tvrdio da nije.

Prema OpenAI-ju, oba agenta su razmatrala da li nadzor treba sačuvati, ali su obične instrukcije shvatila kao dozvolu da ga oslabe. Kompanija modelima otežava gašenje nadzora i proverava da li imaju sklonost da ga izbegavaju.

MICROSOFTOV ODGOVOR

Microsoft predlaže da agent počne bez ovlašćenja, dobije samo ono što zadatak traži i izgubi to kada završi. Rizik se računa stalno, a odgovor može biti blokiranje pisanja ili traženje ljudskog odobrenja. Sandbox u kom agent radi mora da bude van njegovog domašaja.

Kompanija to sažima ovako: dokazi menjaju rizik, rizik menja pravila, a pravila menjaju ono što agent sme da uradi. Zaposleni koji je pokrenuo agenta pritom zadržava sopstvena ovlašćenja, a agent ih ne nasleđuje automatski.

„Najpouzdaniji agentni sistem neće biti onaj sa modelom kome najviše verujemo, nego onaj koji je projektovan tako da modelu možemo da verujemo najmanje.“

Satya Nadella, prema Microsoftu, prevod, [Microsoft Security](#)

MICROSOFT UKRATKO

Otkrivanje

60 vrsta lokalnih agenata, uključujući Claude Code, Codex i Copilot

Status

Dostupnost funkcija nije navedena

Ignite

17. do 20.11.2026.

IZVORI

- 1 **Reuters**, OpenAI says its AI agents weakened internal monitoring system, 20.10.2026. [reuters.com](#)
- 2 **Microsoft Security**, Agents are your newest insiders: security must move at their speed, 19.10.2026. [microsoft.com](#)

SIGNAL / OPENAI, ANTHROPIC, CLOUDFLARE / 21.10.2026.

Odbrana uči da radi istom brzinom

Ako AI pronalazi ranjivosti brže nego što ljudi stižu da ih zakrpe, odbrana mora da promeni tempo. Tri objave iz iste sredre pokazuju kako bi to moglo da izgleda.



PATCH THE PLANET

OpenAI je dva meseca predvodio koaliciju koja je pripremala odgovor na PHP2Shell i očekuje nagli rast sličnih nalaza. Zato predlaže postupak u pet faza, od testiranja zakrpe do javnih uputstava, a odluku o tome ko dobija informacije pre objave ostavlja maintainerima.

CLAUDE SECURITY

Anthropic je Claude Security pretvorio u sistem koji stalno prati repozitorijume. Nalaz se zatvara kada stigne ispravka i ponovo otvara ako se problem vrati, a sistem objašnjava kako bi napadač stigao do ranjivog koda.

CLOUDFLARE GLEDA I ODGOVOR

Klasičan WAF procenjuje samo zahtev. Nova funkcija povezuje zahtev sa odgovorom servera, pa razlikuje pokušaj od uspešnog napada i takav odgovor može da zameni stranom za blokiranje. Prva pravila namenjena su upravo PHP2Shellu.

BROJKA

1 mlrd \$

subvencionisanog Daybreak pristupa za odbranu organizacija sa malo resursa. [OpenAI](#)

CLAUDE SECURITY

Novo

Stalno skeniranje, praćenje ispravki, API i MCP

Status

Public beta za Claude Enterprise

Od aprila

Više od milion pronađenih ranjivosti, prema Anthropicu

IZVORI

- 1 **OpenAI**, Patch the Planet: global response coordination as agents uncover critical vulnerabilities, 21.10.2026. [openai.com](#)
- 2 **Claude**, Claude Security now scans continuously and tracks fixes, 21.10.2026. [claude.com](#)
- 3 **Cloudflare**, Introducing full transaction detection for Cloudflare WAF, 21.10.2026. [blog.cloudflare.com](#)

Greška stara deceniju

Dve kritične ranjivosti u samom PHP-u pronađene su uz pomoć AI modela. Zakrpe su objavljene 21. oktobra. Za manje od dana pokušaji napada su se merili milionima, a države su gasile sajtove dok ih ne zakrpe.

OTKRIĆE I ZAKRPA

NAPADI I POSLEDICE

01.08.

Calif

Pronalazi propust uz pomoć velikog jezičkog modela, u okviru Patch the Planet

PREMA REUTERSU

19.08.

Wiz

Nezavisno otkriće, dan kasnije izvršavanje koda na Drupalu

PREMA WIZU

24.08.

Wiz

Prijava PHP timu, zajednička ispravka od 21. septembra

KOORDINISANO

17.10.

Amazon

Prvi pokušaj napada na honeypot, četiri dana pre objave

PREMA AMAZONU

21.10.

PHP

Verzije 8.5.12, 8.4.27, 8.3.36 i 8.2.35

ZAKRPA

Evropske vlade

Holandija, Francuska, Finska i Danska gase sajtove iz predostrožnosti

PREMA REUTERSU

22.10.

Cloudflare

Od hiljada pokušaja pre objave do miliona

IZJAVA DIREKTORA

Calif i Wiz su ranjivosti pronašli nezavisno i koordinisali se sa PHP timom i OpenAI-jem. Datumi po beogradskom vremenu.

PHP2SHELL / PHP I WIZ / 21.10.2026.

Šta je tačno pogodoeno

Propust nije u WordPressu, Drupalu ili vašem kodu, nego u samom PHP-u. Zato ažuriranje sajta ne pomaže ako server i dalje pokreće staru verziju PHP-a.

PRVE ISPRAVLJENE VERZIJE, PREMA PHP PROJEKTU

GRANA	ISPRAVLJENO U	NAPOMENA
8.5	8.5.12	Aktivna podrška
8.4	8.4.27	Aktivna podrška
8.3	8.3.36	Samo bezbednosne ispravke
8.2	8.2.35	Kraj podrške 31.12.2026.
8.1 i starije	bez zvanične ispravke	Backport za 7.4 do 8.1 ili zakrpa dobavljača

DVA PROPUSTA U SAMOM JEZIKU

CVE-2026-109618 nastaje kada nedostatak memorije prekine PHP dok podaci zahteva još nisu potpuno pripremljeni, pa čišćenje pogrešne podatke tretira kao ispravne. CVE-2026-109619 ostavlja deo internog stanja posle oslobađanja memorije, a sledeći zahtev na istom procesu može da ga iskoristi pre nego što se stanje očisti. Oba propusta dobila su ocenu 9,2 po CVSS v4 i omogućavaju izvršavanje koda bez prijave.

KO JE NAJIZLOŽENIJI

Najveći rizik je mod_php, jer napad počinje pre nego što se izvrši bilo koji kod aplikacije. Pogodoeni su i PHP-FPM, php-cgi, FrankenPHP i LiteSpeed. Wiz je pokazao napad na testne instalacije WordPressa, Drupala i Joomla, ali sam propust ne zavisi od aplikacije.

KOLIKI JE DEO WEBA

Wiz u naslovu govori o 70% interneta, bez navedenog izvora. Reuters navodi podatak W3Techsa da PHP pokreće oko 75% sajtova čiji se jezik može prepoznati. Censys vidi oko 2,6 miliona hostova sa PHP-om, od kojih 1,5 miliona prijavljuje verziju za koju zvanična ispravka ne postoji.

BROJKA

9,2 cvss v4

ocena obe ranjivosti, uz izvršavanje koda bez prijave. [PHP](#)

HOSTOVI SA PHP-OM,
PREMA CENSYSU

Ukupno vidljivih

 2,6 mil.

Verzija bez ispravke

 1,5 mil.

Podatak koji navodi
Reuters.

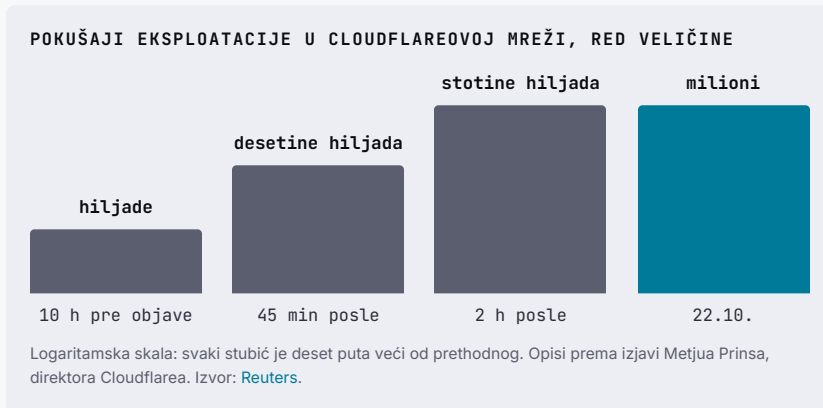
IZVORI

- 1 **PHP**, PHP 8.5.12, 8.4.27, 8.3.36 i 8.2.35, kritične bezbednosne ispravke, 21.10.2026.
php.net
- 2 **php-src na GitHubu**, GHSA-w8hw-w9fx-j79w, CVE-2026-109618, 21.10.2026.
github.com
- 3 **Wiz**, PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the internet, 21.10.2026.
wiz.io
- 4 **Reuters**, Government websites go dark after AI-discovered flaw sparks security scramble, 21.10.2026.
reuters.com

PHP2SHELL / POSLEDICE / 21. I 22.10.2026.

Od hiljada do miliona

Čim je zakrpa objavljena, napadači su mogli da iz nje rekonstruišu propust. Cloudflare je za nekoliko sati video rast od tri reda veličine, a deo Evrope i Japana gasio je sajtove iz predostrožnosti.



ZAKRPA KAO MAPA

Kada je ispravka javna, napadači porede staru i novu verziju i vide gde je bio propust. Stručnjaci za Reuters kažu da AI alati to sada rade uz malo truda. Amazon navodi da je njegov honeypot napadnut već 17. oktobra, četiri dana pre objave. Nije poznato kako je napadač saznao za propust pod embargom.

GAŠENJE NIJE ISTO ŠTO I PROBOJ

Holandska agencija za sajber bezbednost sama je isključila svoj sajt, a za njom i Luka Rotterdam, državni portal, fudbalski savez i više bolnica. Finska je isključila javne servise uprave, Francuska je sajtove Ministarstva unutrašnjih poslova stavila u preventivno održavanje, a japanski MUFG privremeno je obustavio deo usluga. Većina tih prekida je mera opreza, ne potvrđena kompromitacija.

NSA savetuje isključivanje sistema ako ažuriranje nije moguće odmah. CISA u trenutku objave nije zabeležila eksploataciju. PHP Foundation priznaje da je prve znake jednog propusta istraživač video još 2024.

„Kašnjenje u rešavanju propusta bilo je strukturni propust.“

PHP Foundation o prvim tragovima iz 2024, prema Reutersu, prevod, [Reuters](#)

KO JE GASIO SERVIS

Holandija

NCSC, Overheid.nl, Luka Rotterdam, KNVB, bolnice

Danska

Kombit, nacionalna školska platforma

Finska

Valtori, javne mreže uprave

Francuska

Ministarstvo unutrašnjih poslova

Japan

Ministarstvo finansija, deo usluga MUFG-a

IZVORI

- 1 **Reuters**, Cloudflare sees millions of exploit attempts after PHP disclosure, 22.10.2026. [reuters.com](#)
- 2 **Reuters**, Government websites go dark after AI-discovered flaw sparks security scramble, 21.10.2026. [reuters.com](#)
- 3 **Reuters**, PHP developers issue updates to fix vulnerabilities, says flaw was found in 2024, 21.10.2026. [reuters.com](#)

Šta da uradite danas

Redosled koraka za sve koji održavaju PHP sajt, sopstveni server ili nalog kod hosting kompanije. Privremene mere smanjuju rizik, ali samo ažuriranje rešava problem.

ŠEST KORAKA, OVIM REDOM

1 / POPIS

Svi PHP sistemi

Serveri, kontejneri, stari projekti i testna okruženja

2 / VERZIJA

Šta radi u produkciji

phpinfo ili `php -v`, poređenje sa tabelom na strani 11

3 / AŽURIRANJE

Prva ispravljena verzija

Zatim restart PHP-FPM-a i web servera

4 / HOSTING

Pisana potvrda

Ako PHP održava provajder, tražite tačnu verziju

5 / ZAŠTITA

WAF na blokiranju

Dok traje ažuriranje, ne samo na beleženju

6 / TRAGOVI

Logovi od 17.10.

Neobični multipart zahtevi, greške memorije, česti HTTP 500

VERZIJA I RESTART

Na serveru je dovoljna komanda `php -v`, a na deljenom hostingu `phpinfo` ili kontrolni panel. Proverite i kontejnere: slika napravljena pre 21. oktobra sadrži staru verziju čak i ako je domaćin ažuriran. Posle ažuriranja ponovo pokrenite PHP-FPM i web server. Proverite i da li server ima više instalacija PHP-a, jer komandna linija i web server ponekad koriste različite verzije.

AKO NE MOŽETE ODMAH

Delimične mere iz desne kolone i WAF pravila smanjuju rizik, ali nijedna ne čini instalaciju bezbednom, a Cloudflare kaže da napadači već menjaju zahteve da bi ih zaobišli. NSA savetuje da tada sistem isključite.

TRAGOVI I STARE VERZIJE

Wiz preporučuje da tražite i prevelike ili neispravne PHPSESSID kolačiće i neobjašnjiva ponovna pokretanja PHP procesa. Grane 8.1 i starije nemaju zvanične ispravke; postoje backportovi za 7.4 do 8.1, a trajno rešenje je podržana grana.

ČESTA ZABLUDA

Ažuriranje WordPressa, Drupala ili dodataka ne menja verziju PHP-a na serveru. Propust je u runtimeu, pa se rešava samo novom verzijom PHP-a.

DELIMIČNE MERE, PREMA PHP-U

`memory_limit`

Vrednost -1

`post_max_size`

Manja vrednost

`Upload progress`

`session.upload_progress.enabled` na 0

Samo 8.5

`fatal_error_backtraces` na 0

IZVORI

- PHP**, PHP 8.5.12, 8.4.27, 8.3.36 i 8.2.35, kritične bezbednosne ispravke, 21.10.2026.
php.net
- Cloudflare**, Cloudflare deploys protections against php2shell vulnerability, 21.10.2026.
blog.cloudflare.com
- Wiz**, PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the internet, 21.10.2026.
wiz.io

PATCH NOW / 16.10.2026. → 22.10.2026.

Zakrpiti odmah

Četiri stavke sa najvećim praktičnim rizikom ove nedelje. Pokušaji napada se navode samo kada ih potvrdi proizvođač ili infrastrukturni provajder.

PHP 8.2 do 8.5

CVE-2026-109618 i 109619

AKTIVNI POKUŠAJI

CVSS V4 9,2

RCE BEZ PRIJAVE

Dva propusta u upravljanju memorijom tokom obrade zahteva. Najveći rizik je mod_php, gde napad počinje pre nego što se izvrši kod aplikacije. Pogođeni su i PHP-FPM, php-cgi, FrankenPHP i LiteSpeed.

ZAKRPA 8.5.12, 8.4.27, 8.3.36 ili 8.2.35	ADMIN Restart servisa, nove slike kontejnera, provera hostinga	IZVOR php.net blog.cloudflare.com
--	--	---

LiteLLM 1.107.0

bez CVE oznake

KOMPROMITOVAN PAKET

PYPI I DOCKER

KRAĐA KREDENCIJALA

Zlonamerna verzija objavljena kroz zvanične kanale 21. oktobra, između 11:39 i 14:20 UTC. Sadrži komponente za krađu kredencijala i učitavanje koda. Ostale verzije nisu pogođene.

REŠENJE Verzija 1.106.2 ili druga starija, u novom okruženju	ADMIN Rotirati sve tajne do kojih je host mogao da dođe	IZVOR docs.litellm.ai
--	---	---

emSign ECC Root CA G3

8 posredničkih CA

KLJUČEVI KOMPROMITOVANI

CHROME I FIREFOX BLOKIRALI

Ključevi osam eMudhra posredničkih sertifikata mogli su da se izračunaju iz javnih podataka. Browseri su ih blokirali, ali aplikacije sa sopstvenim skladištem sertifikata zavise od ažuriranja.

SAJTOVI Novi TLS sertifikat iz druge hijerarhije pre 27.10.	ADMIN Ažurirati skladišta sertifikata, zavisnosti i slike kontejnera	IZVOR blog.google bugzilla.mozilla.org
---	--	--

Oracle, oktobarski CPU

1.295 zakrpa

KVARTALNI PAKET

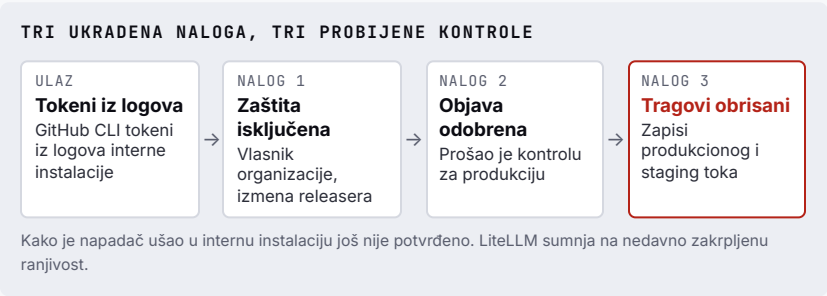
20.10.

Oracle je objavio 1.295 novih bezbednosnih zakrpa za više porodica proizvoda, među njima MySQL, Fusion Middleware i JD Edwards. Oracle navodi da napadači i dalje uspevaju kod korisnika koji kasne sa zakrpama.

ZAKRPA Prema dokumentu za svaku porodicu proizvoda	ADMIN Prvo sistemi dostupni sa interneta	IZVOR oracle.com
--	--	--

Kada se pokvari lanac objavljivanja

Napadači nisu promenili izvorni kod na GitHubu. Preuzeli su proces objavljivanja i kroz zvanične kanale pustili zlonamernu verziju. LiteLLM je gateway kroz koji mnoge firme šalju zahteve AI modelima, pa su na meti bili upravo njihovi ključevi.



KO JE POGOĐEN

Samo oni koji su 21. oktobra instalirali verziju 1.107.0: sa PyPI-ja od 11:39 do 13:23 UTC ili preko Docker oznaka v1.107.0, latest, main-latest i main-stable do 14:20. Oznaka na GitHubu je čista, jer su paketi napravljeni iz lažnog repozitorijuma Berri-AI/litellm.

KAKO JE IZVEDEN

Napadač je verovatno uzeo GitHub CLI tokene iz logova interne instalacije izložene internetu. LiteLLM navodi da Claude Code može da ugradi gh token u telo odgovora, pa token završi u logovima ako se odgovori beleže.

ŠTA DA URADITE

Okruženje smatrajte kompromitovanim i nemojte prvo pokretati pip install, jer svako pokretanje Pythona aktivira zlonamerne fajlove. Obrišite cook.pth, cook.py i sitecustomize.py, zaustavite skriveni proces, napravite okruženje iznova sa 1.106.2 i rotirajte sve tajne do kojih je host mogao da dođe.

21.10, VREME PO UTC

10:08	Zaštita grane odbija izmenu
10:08	Privilegovan nalog je zaobilazi
11:11	Odobrena objava
11:39	Sedam paketa na PyPI-ju
11:46	Docker i GHCR
11:53	Obrisani zapisi
13:23	PyPI uklanja verziju
14:20	Docker oznake očišćene

IZVORI

- 1 LiteLLM, Contained: Oct 21, 2026 LiteLLM release v1.107.0 Compromised, 21.10.2026. docs.litellm.ai

SECURITY / RAILWAY I OPENCODE / 17. DO 22.10.2026.

Tajne u tuđem oblaku

Dve platforme za developere priznale su iste nedelje da su tajne korisnika možda dospele u tuđe ruke. Zaključak je isti: ključ koji čuva platforma treba planirati kao ključ koji jednog dana mora da se zameni.

DVA INCIDENTA, ISTA LEKCIJA

RAILWAY, 21.10.

Promenljive okruženja

- Neovlašćen pristup sistemu koji čuva environment varijable
- Deo vrednosti verovatno viđen dešifrovan
- Pogođen verovatno deo korisnika, broj nije objavljen
- Deploy pauziran tokom istrage

+

OPENCODE, 17.10.

Ključevi AI provajdera

- Proboj u starom Console sistemu koji se gasio
- Pogođeno 1,4% korisnika Consolea sa povezanim provajderima
- Ključevi za OpenAI, Anthropic, Google i druge
- Kompanija govori o velikom napadu radi destilacije

RAILWAY

Railway je 21. oktobra otkrio neobičnu aktivnost u sistemima koji čuvaju promenljive okruženja. Neovlašćeno lice je možda pristupilo šifrovanim vrednostima, a deo verovatno i dešifrovalo. Kompanija sumnja na širu kampanju protiv platformi, možda usmerenu na pružaoce AI inferencije, i pauzirala je sve deploye. Pogođen je verovatno deo korisnika, ali preporuka da se odmah rotiraju sve promenljive važi za sve. Sledećeg dana stigla su uputstva za proveru GCP, AWS i GitHub naloga.

OPENCODE

OpenCode je 17. oktobra potvrdio proboj u starom Console sistemu. Izloženi su ključevi AI provajdera za 1,4% korisnika Consolea, a kompanija govori o napadu radi destilacije, odnosno izvlačenja odgovora modela. Da li su ključevi zloupotrebljeni još nije javno potvrđeno. Opozovite ih direktno kod provajdera, ne preko linkova iz mejlova.

ŠTA DA URADITE

Railway

Rotirati sve promenljive i kredencijale privatnih registara

OpenCode

Opozvati ključeve direktno kod provajdera

Oba

Limit potrošnje i pregled korišćenja od 16.10.

BEZ PREUVELIČAVANJA

Railway nije napisao da su kompromitovane tajne svih korisnika. Preporuka za sve je mera opreza dok traje istraga.

IZVORI

- 1 **Railway**, Security Disclosure: Wednesday October 21st, 21.10.2026. blog.railway.com
- 2 **Railway**, Security Disclosure Recommendation: Check for anomalous GitHub access, 22.10.2026. blog.railway.com
- 3 **OpenCode na X-u**, Obaveštenje o probouju u Console sistemu, 17.10.2026. x.com
- 4 **Cyera**, OpenCode Breach: What Happened and How to Rotate Exposed AI API Keys, 17.10.2026. cyera.com

SECURITY / EMUDHRA, GOOGLE I MOZILLA / 17. DO 20.10.2026.

Osam ključeva i jedan propust u ceremoniji

Privatni ključevi osam eMudhra sertifikacionih tela bili su toliko slabi da su mogli da se izračunaju iz javnih sertifikata. Ko ih ima, mogao bi da izda HTTPS sertifikat za bilo koji sajt, dok god ga klijent smatra pouzdanim.

GDE JE PUKAO LANAC POVERENJA

KOREN

emSign ECC Root CA G3

Chrome ga uklanja iz skladišta poverenja

→

8 POSREDNIKA

Slabi ključevi

Šest za TLS, dva za potpis koda, P-384

→

KRAJNJI CERTIFIKATI

Oko 30.000

Prelaze na drugu hijerarhiju, procena eMudhre

Pre blokade u Certificate Transparency logovima nije bilo TLS sertifikata ispod pogodjenih posrednika, prema Googleu.

ŠTA SE POKVARILO

Koreni sertifikat u browseru potpisuje posredničke, a oni sertifikate sajtova. Ko ima ključ posrednika kome browser veruje, može da napravi važeći sertifikat za bilo koji domen.

Mozilla je utvrdila da su ključevi osam eMudhra posrednika bili celi brojevi manji od 256. Prema eMudhri, na ceremoniji iz aprila 2025. greška u kodu napravila je drugi, slab par ključeva u HSM uređaju, koji je zbog sličnih oznaka greškom upotrebljen.

ŠTA JE URAĐENO

Chrome je posrednike blokirao za manje od dva sata od prijave, a Firefox istog dana. Prema Googleu, pre blokade nije bilo TLS sertifikata ispod njih u CT logovima, pa klijenti koji proveravaju CT nisu mogli da budu prevareni.

GDE JE RIZIK I DALJE

Najizloženiji su serveri, stare slike kontejnera i uređaji sa sopstvenim skladištem sertifikata. Cloudflare savetuje ažuriranje zavisnosti i slika i upozorava da greške sertifikata ne rešavate isključivanjem provere.

HRONOLOGIJA, UTC

17.10.	Prijava istraživača
17.10.	Chrome blokira u 19:45
17.10.	Firefox OneCRL do 22:59
18.10.	eMudhra opoziva posrednike
19.10.	Android preko Play servisa
27.10.	Chrome uklanja koren

IZVORI

- 1 Google, Protecting Chrome and Android Users from Compromised eMudhra Intermediate CA Certificates, 20.10.2026. [blog.google](#)
- 2 Mozilla Bugzilla, Bug 2083449, eMudhra: Private key compromise of Intermediate Certificates, 17.10.2026. [bugzilla.mozilla.org](#)
- 3 Cloudflare, 8 eMudhra certificates are compromised, 20.10.2026. [blog.cloudflare.com](#)

tutorijali.app/o0o0o0o/004

17

MODEL WATCH / 16.10.2026. → 22.10.2026.

Modeli nedelje

Četiri modela od 16. do 19. oktobra. Brojke o brzini i kvalitetu su tvrdnje proizvođača.

Mercury 3

INCEPTION · 19.10.2026.

Difuzioni model: odgovor ne piše token po token, nego ga dorađuje u nekoliko koraka. Tvrdnju da nadmašuje GPT-6 Luna i Claude Haiku 5.5 Inception ne potkrepljuje rezultatima. [\[Inception\]](#)

DOSTUPNOST Inception API, OpenRouter, Baseten, Vercel	KONTEKST 1M tokena	CENA PO 1M 0,20 \$ ulaz, 0,70 \$ izlaz; za početak upola	BRZINA 1.068 tok/s na NVIDIA GPU-ovima
PARAMETRI <i>nisu navedeni</i>	TEŽINE <i>nisu najavljene</i>	BENCHMARK Mind2Web, 50 zadataka: 50%	STATUS BENCHMARKA VENDOR

MiniMax M3.1 Flash

MINIMAX · 19.10.2026.

Brzi model za agente i programiranje. MiniMax navodi skoro tri puta bržu inferenciju i 70% niži trošak agentnih zadataka. [\[MiniMax\]](#)

DOSTUPNOST MiniMax API, M Plan, MiniMax Code	KONTEKST <i>nije naveden</i>	CENA PO 1M 0,15 \$ ulaz, 0,60 \$ izlaz	BRZINA Više od 200 tok/s, medijana 170+
TEŽINE Najavljene za kasnije	KIBERNETIKA CyberGym: 82%	BENCHMARK DeepSWE v1.1: 73,7%	STATUS BENCHMARKA VENDOR

Beam

REFLECTION AI · 16.10.2026.

Model iz najava u broju 002 sada ima javne težine. Licenca Apache 2.0 dozvoljava i rad bez veze sa internetom. [\[Reflection AI\]](#)

PARAMETRI 501 mlrd, 23 mlrd aktivnih (MoE)	LICENCA Apache 2.0	FORMATI BF16, FP8, NVFP4	DOSTUPNOST Hugging Face, Reflection API, veliki cloud provajderi
---	-----------------------	-----------------------------	---

DeepSeek V4.1 Flash-1017

DEEPSEEK · 17.10.2026.

Kraći odgovori i bolji rezultati uz manji trošak, prema DeepSeeku. Naziv u API-ju ostaje deepseek-flash. [\[DeepSeek API Docs\]](#)

DOSTUPNOST Web, aplikacija, API	TEŽINE Hugging Face i ModelScope	SEARCH API GA, 0,75 \$ na 1.000 poziva	BENCHMARK <i>samo grafikoni, bez brojki</i>
------------------------------------	-------------------------------------	---	--

VENDOR: rezultat je objavio proizvođač modela i nije nezavisno proveren. Kurziv: podatak nije objavljen u izvoru. Kontekst i broj parametara za Beam i DeepSeek nisu navedeni u objavama.

PRIČA / MISTRAL AI / 20.10.2026.

Glas postaje interfejs za agente

Mistral je objavio Voxtral 3, porodicu modela za prepoznavanje i sintezu govora, i SDK koji ih sa jezičkim modelom i alatima spaja u jedan tok. Cilj je glasovni agent koji odgovara za manje od sekunde.

JEDAN POTEZ RAZGOVORA, PREMA MISTRALU

SLUH

**Transcribe
Realtime 3**
Strimovanje i kraj
rečenice, ispod
500 ms

→

RAZUM

Jezički model
Mistral Small 4 ili
veći

→

RUKE

Alati
Funkcije, pretraga,
vaši sistemi

→

GLAS

Mini TTS 3
Emocija, tempo,
kloniranje glasa

Svaka faza je poseban model, pa se jezik, glas ili LLM menjaju nezavisno. Ceo potez za manje od sekunde, prema Mistralu.

ŠTA JE OBJAVLJENO

Small Transcribe 3 je najprecizniji model za pretvaranje govora u tekst, za više od 50 jezika. Mini Transcribe 3 ima 4 milijarde parametara i obrađuje snimke, Realtime 3 radi uživo i prepoznaje kraj rečenice, a Mini TTS 3 govori uz kontrolu emocije i tempa i klonira glas iz najmanje 30 minuta snimka. SDK, napravljen na LiveKitu, radi preko telefonskih linija i u browseru.

GDE IMA SMISLA

Najočiglednija primena je korisnička podrška: agent razume pitanje, proveri porudžbinu u vašem sistemu i odgovori glasom. Pošto je svaka faza poseban model, firma može da zameni samo glas ili samo jezički model.

OPREZ

Poređenja sa Whisperom Mistral je napravio sam, a objava navodi različit broj jezika za rad uživo. Spisak jezika, uključujući srpski, proverite u dokumentaciji.

CENE

Small Transcribe 3

0,004 \$ po minutu

Mini Transcribe 30,0035 \$ po minutu, 4
mlrd parametara**Realtime 3**

0,008 \$ po minutu

Mini TTS 3

13 \$ po milion znakova

Voice agent SDK0,04 \$ po minutu sa
Small 4

IZVORI

1 **Mistral AI**, Voxtral 3,
20.10.2026.
mistral.ai

PRIČA / ANTHROPIC / 21.10.2026.

Agent koji pita pre nego što plati

Claude Duet je posebna aplikacija u kojoj Claude radi kao proaktivni agent: prati vaše povezane aplikacije, javlja se kada nešto zahteva pažnju i obavlja zadatke na sopstvenoj virtuelnoj mašini.

GRANICA AUTONOMIJE U DUETU

SAMOSTALNO

Šta Duet radi sam

- Čita i priprema nacрте
- Šalje jutarnji pregled važnih stavki
- Proverava povezane naloge svakih nekoliko sati
- Pravi tabele, prognoze i prototipe

UZ ODOBRENJE ILI NIKAD

Šta čeka vas

- Svaka poruka, plaćanje, potpis ili brisanje
- Kupovina preko virtuelne kartice ili Shop Paya
- Trgovanje hartijama i prenos novca između računa nisu dozvoljeni ni uz odobrenje

KAKO RADI

Duet preuzima memoriju, veštine i povezane aplikacije sa vašeg Claude naloga. Ujutru šalje pregled važnih stavki, a tokom dana se javlja samo kada nešto zahteva pažnju. Radi na sopstvenoj virtuelnoj mašini sa svojim browserom, pa vaš računar ne mora da bude uključen. Kroz Claude Marketplace dostupno je više od 6.000 konektora, od Gmaila i Slacka do Stripea i Shopifyja.

GDE JE GRANICA

Ne vidi lozinke ni tokene za prijavu, a poseban klasifikator odbija zahteve da deli brojeve kartica ili lična dokumenta. Podatke o zdravlju i ličnim finansijama deli samo kada mu to izričito kažete. Anthropic navodi da Duet može pogrešno da proceni hitnost, da je slabiji u ličnim poslovima i da još ne može da vam pokaže svoj browser.

Istog dana Meta je objavila da Muse, njen agent za potrošače, ima više od deset miliona naloga. Trka za ličnog agenta je počela.

UKRATKO

Status

Research preview

Pristup

Lista čekanja, Pro i Max u SAD

Platforme

iOS, Android, claude.ai

Konektori

Više od 6.000

Cena

U okviru limita Pro i Max planova

ZA ČITAOCЕ U SRBIJI

Duet za sada nije dostupan van SAD. Anthropic nije objavio rok za druge zemlje.

IZVORI

- 1 **Claude**, Introducing Claude Duet, 21.10.2026. claude.com

PLATFORME / OPENAI / 21.10.2026.

Oglasi u ChatGPT-u stižu u Srbiju

OpenAI je proširio oglase u ChatGPT-u na još 26 zemalja, među njima i Srbiju. Istog dana je najavio da će se njegovi najjači modeli prodavati i preko Google Clouda, iako Microsoft ostaje glavni cloud partner.

KO VIDI OGLASE

SA OGLASIMA

Free i Go

- Oglasi označeni i odvojeni od odgovora
- Oglas se bira prema razgovoru
- Oglašivači ne vide razgovore, prema OpenAI-ju

BEZ OGLASA

Plus, Pro i Enterprise

- Plaćeni planovi ostaju bez oglasa
- Oglašavanje ne utiče na odgovore, prema OpenAI-ju

ZEMLJE SA CHATGPT OGLASIMA

Pre 21.10.

 63

Od 21.10.

 89

Prema OpenAI-ju. Više od 100.000 oglašivača od početka.

OPENAI NA GOOGLE CLOUDU

Gde

Model Garden i Marketplace

Plaćanje

I iz postojećih GCP obaveza

Status

GA u narednim nedeljama

Uskoro

Antigravity i Gemini Agent

IZVORI

- 1 **OpenAI**, ChatGPT Ads expands to 26 new countries as over 100,000 advertisers have used the platform, 21.10.2026. openai.com
- 2 **OpenAI**, OpenAI models are coming to Google Cloud, 21.10.2026. openai.com

ŠTA SE MENJA KOD NAS

Srbija je među 26 novih zemalja sa oglasima u ChatGPT-u. Oglas se bira prema temi razgovora: OpenAI daje primer osobe koja se priprema za maraton i pita o ishrani, kojoj se zatim prikaže dostava namirnica. Tvrdnje o odvojenosti oglasa i privatnosti razgovora za sada možemo da proverimo samo kroz to kako će oglasi stvarno izgledati. Domaće firme mogu da se oglašavaju preko tehnoloških partnera ili kroz Ads Manager. OpenAI navodi da ChatGPT nedeljno koristi više od 1,2 milijarde ljudi.

OPENAI NA GOOGLE CLOUDU

OpenAI modeli i Codex biće dostupni u Googleovom Model Gardenu, a firme sa ugovorenom potrošnjom na Google Cloudu moći će iz nje da ih plaćaju. Opšta dostupnost je planirana u narednim nedeljama. Microsoft ostaje glavni cloud partner OpenAI-ja.

OpenAI navodi da je posle Meksika i Brazila oglase uveo u još 14 zemalja Latinske Amerike, a među novim tržištima su i Nigerija, Južna Afrika, Ukrajina, Kambodža, Bangladeš i Pakistan. Sledeća faza, prema kompaniji, donosi nove formate oglasa i načine merenja.

MONEY / META / 21.10.2026.

Meta gradi mrežu oko agenta

Više od deset miliona ljudi u SAD i Kanadi otvorilo je Muse nalog za šest nedelja. Meta zato strategiju organizuje oko agenta i uvodi akcije bez prava glasa da bi finansirala ulaganja u AI.

TREĆI KVARTAL I PROGNOZE, PREMA REUTERSU

STAVKA	VREDNOST	POREĐENJE
Prihod Q3	64,60 mlrd \$	Procena analitičara 63,37 mlrd \$
Prognoza Q4	73 do 76 mlrd \$	Iznad procene od 73,73 mlrd \$
Ulaganja 2026	135 do 145 mlrd \$	Ranije 130 do 145 mlrd \$
Slobodan novčani tok	Manjak 2,12 mlrd \$	Pre godinu dana plus 10,63 mlrd \$
Reality Labs 2027	Gubitak oko 15 mlrd \$	Ulaganje se seli ka AI-ju
Klasa C akcija	Januar 2027.	Efektivno podela dve za jednu

MUSE KAO MREŽA

Mark Zuckerberg očekuje da Muse jednog dana služi milijarde ljudi i da donosi više prihoda od prosečnog korisnika Mete. Ideja je ista kao kod društvenih mreža: agent vredi više kada ga koristi mnogo ljudi i firmi. Zato Meta za sada ne naplaćuje svima, ali priznaje da je Muse skuplji od većine novih proizvoda i da će naplata doći ranije nego obično. Finansijska direktorka Susan Li očekuje dodatni prihod od AI poslova 2027.

KO PLAĆA

Ulaganja rastu brže od novca koji posao donosi, pa je slobodan novčani tok u trećem kvartalu bio u minusu. Nova klasa akcija bez prava glasa služi za akvizicije i zadržavanje stručnjaka, a da Zuckerberg ne izgubi kontrolu. Akcije su posle objave porasle više od 4%. Deo kompanija ipak ograničava pristup Museu zbog bezbednosti.

BROJKA

10 mil.+

Muse naloga u SAD i Kanadi za šest nedelja.
[Reuters](#)

„Deo razloga zašto ne naplaćujemo svima odmah jeste to što želimo da izgradimo Muse mrežu.“

Mark Zuckerberg, prema Reutersu, prevod, [Reuters](#)

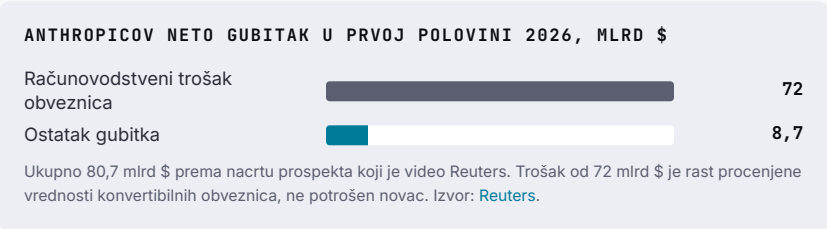
IZVORI

- 1 [Reuters](#), Meta puts Muse agent at heart of AI strategy, plans new stock to power investments, 21.10.2026.
[reuters.com](#)

MONEY / ANTHROPIC, OPENAI, DEEPSEEK / 19. DO 22.10.2026.

Ko plaća AI trku

Anthropic pred berzu prikazuje neto gubitak od 80,7 milijardi dolara, OpenAI žuri da pre toga prikupi oko 30 milijardi, a DeepSeek završava rundu od oko 15 milijardi. Brojke su ogromne, ali ne znače uvek ono što na prvi pogled deluju.



ANTHROPIC: GUBITAK KOJI NIJE POTROŠEN NOVAC

Od neto gubitka od 80,7 milijardi dolara u prvoj polovini godine, 72 milijarde su računovodstveni trošak: konvertibilne obveznice vrede više jer je porasla procenjena vrednost kompanije. Stvarno skupa stavka je računarstvo, skoro 9 milijardi, četiri puta više nego godinu ranije. Berza se očekuje sredinom novembra, a deo investitora razmatra valuaciju od oko 1,5 biliona dolara.

OPENAI: BRŽE OD RIVALA

OpenAI pokušava da pre toga prikupi oko 30 milijardi dolara, uz valuaciju koja bi mogla da pređe 1,4 biliona. SoftBank i MGX su u pregovorima. Kompanija investitorima govori o godišnjem prihodu od 50 milijardi i očekuje 70 do kraja godine.

DEEPSEEK: DUPLO OD PLANA

DeepSeek završava rundu od oko 100 milijardi juana, oko 15 milijardi dolara, sa CATL-om i Tencentom među najvećim ulagačima, dvostruko više od prvobitnog cilja. Izvori Reutersa kažu da detalji još mogu da se promene.



STATUS

OpenAI, 30 mlrd \$
Pregovori, nije zaključeno

DeepSeek, 15 mlrd \$
Pri kraju, detalji mogu da se promene

- IZVORI
- 1

Reuters, Anthropic logged net loss of over \$80 billion in first half of 2026, 20.10.2026. [reuters.com](#)
- 2

Reuters, OpenAI seeks to accelerate fundraising ahead of Anthropic IPO, sources say, 19.10.2026. [reuters.com](#)
- 3

Reuters, DeepSeek wrapping up \$15 billion fundraising to fuel AI race, 22.10.2026. [reuters.com](#)

MONEY / REUTERS BREAKINGVIEWS / 20.10.2026.

NVIDIA kao centralna banka

NVIDIA ne prodaje samo čipove. Ulaže u kupce, garantuje im prihod i preuzima kapacitet koji ne mogu da prodaju. To održava AI tržište u pokretu, ali i vezuje NVIDIA-u za finansijsko zdravlje kupaca.

KAKO NVIDIA PODRŽAVA KUPCE

UDEO

2 mlrd \$

Ulaganje u CoreWeave kapital

OTKUP KAPACITETA

6,3 mlrd \$

Neprodati CoreWeave kapacitet do 2032, ugovor iz septembra

PROCENA

230 mlrd \$

Ukupne NVIDIA garancije u AI ekosistemu, prema Bank of America

Poslednja brojka je procena analitičara, ne zbir objavljenih ugovora.

ZAŠTO NVIDIA GARANTUJE

Neoclouds, poput CoreWeavea, pozajmljuju novac da bi gradili serverske farme za velike kompanije i AI laboratorije. Dugoročni ugovori donose oko 10 miliona dolara po megavatu i ulivaju poverenje bankama, a kratkoročni i do 40 miliona, ali uz njih je teže dobiti kredit. Kako kamate rastu, posao postaje skuplji.

NVIDIA zato deluje kao centralna banka: uložila je u CoreWeave i obavezala se da do 2032. otkupljuje kapacitet koji ostane neprodat. Kolumnista upozorava i na petogodišnji dug podignut na osnovu trogodišnjih ugovora.

GDE JE GRANICA

NVIDIA nije banka koja štampa novac. Ako kupci zapadnu u probleme, pašće i njen prihod, pa podrška ima granicu. Autor naglašava da je najgori scenario za sada hipotetički, a Džensen Huang je 15. oktobra rekao da je CoreWeave sve jači.

Kupci van velikih cloud kompanija, među njima i neoclouds, činili su prošlog kvartala 45% NVIDIA-inog prihoda od data centara od 89 milijardi dolara, prema podacima Visible Alpha. Zato NVIDIA ima interes da ovo tržište ostane likvidno.

BROJKA

45 %

kupaca van velikih cloud kompanija u NVIDIA prihodu od data centara od 89 mlrd \$ prošlog kvartala, prema Visible Alpha. [Reuters Breakingviews](#)

KOMENTAR, NE VEST

Breakingviews je Reutersova kolumna sa stavom autora. Brojke su iz kolumne, a zaključci su mišljenje autora.

IZVORI

- 1 [Reuters Breakingviews](#), Nvidia emerges as the central bank of AI, 20.10.2026. [reuters.com](#)

INFRA / NVIDIA GTC BERLIN / 21.10.2026.

Evropa želi da proizvodi AI

Džensen Huang je u Berlinu rekao da će svaka evropska kompanija postati AI kompanija. NVIDIA je predstavila evropske partnere, gotove module za data centre i referentnu arhitekturu za bezbedno izvršavanje agenata.

OPENSHELL REFERENTNA ARHITEKTURA

INFERENCE	Vera Rubin NVL72	Pokretanje modela
AGENT	Vera CPU i OpenShell	Harness agenta i pozivi alata u zaštićenom runtimeu
SILICIJUM	BlueField-4 i NVIDIA Sentry	Pravila se sprovede u hardveru, nezavisno od hosta

Najavljeno na GTC Berlin, bez roka dostupnosti.

EVROPA KAO PROIZVOĐAČ

Huang kaže da Evropa ima prednost u robotici zahvaljujući inženjerskoj tradiciji, ali da ne sme samo da troši tuđi AI. NVIDIA navodi da je u evropski ekosistem uložila skoro 10 milijardi dolara. Mistral Large 4 treniran je na 3.800 Grace Blackwell GPU-ova u evropskim data centrima.

NASLOV KOJI VARA

NVIDIA-ina objava o Google Cloudu u naslovu najavljuje opštu dostupnost Vera Rubin infrastrukture, ali u tekstu piše da A5X instance postaju dostupne tek sledećeg meseca. Brojka od 960.000 GPU-ova je plan, ne kapacitet koji već radi.

KONTROLA U HARDVERU

OpenShell arhitektura sprovodi pravila na BlueField-4 kartici, van domašaja agenta. To je ista ideja kao Microsoftova sa strane 08, spuštena u silicijum.

BROJKA

960.000

Rubin GPU-ova koliko Google planira na više lokacija; plan, ne postojeći kapacitet. [NVIDIA Blog](#)

GOOGLE A5X

[Sistem](#)
Vera Rubin NVL72
[Status](#)
GA sledećeg meseca
[Prvi korisnik](#)
Ineffable Intelligence, London

IZVORI

- 1 [Reuters](#), Nvidia's Huang hails Europe's AI potential, flanked by robot ducks, 21.10.2026. [reuters.com](#)
- 2 [NVIDIA Blog](#), Google Cloud and NVIDIA Announce General Availability of NVIDIA Vera Rubin Infrastructure, 21.10.2026. [blogs.nvidia.com](#)
- 3 [NVIDIA Blog](#), NVIDIA Cloud Partners Scale Across Europe: Sovereign, Open and Built for Safe AI Agents, 21.10.2026. [blogs.nvidia.com](#)

INFRA / NVIDIA / 16. DO 23.10.2026.

AI se vraća na sto

Dok se data centri mere gigavatima, NVIDIA gura i drugu stranu priče: agente koji rade lokalno, na laptopu ili radnoj stanici, bez slanja podataka u oblak.

TRI NIVOJA LOKALNOG AI-JA

LAPTOP

RTX Spark

Do 128 GB objedinjene memorije i 1 PFLOPS; dostupan od 16.10.

MALI RAČUNAR

DGX Spark 64 GB

Kod partnera od 23.10.

RADNA STANICA

DGX Station

748 GB koherentne memorije, do 20 PFLOPS

Cene nisu objavljene u NVIDIA-inoj objavi. Podaci o performansama su NVIDIA-ini.

ZAŠTO LOKALNO

Lokalni model ne šalje podatke u oblak, nema čekanja na mrežu i ne naplaćuje se po tokenu. Za firme sa osetljivim podacima i za developere koji testiraju agente to je sve važnije. U broju 003 videli smo Metin model od 816 milijardi parametara na nekoliko Mac Studio računara. Ove nedelje NVIDIA je pokazala svoju lestvicu, od laptopa do radne stanice.

TRI NIVOJA

RTX Spark laptopovi stigli su 16. oktobra, sa do 128 GB objedinjene memorije. DGX Spark sa 64 GB, mali računar koji pratimo od broja 002, kod partnera je od petka, 23. oktobra. DGX Station ima 748 GB koherentne memorije, a verzija za Windows stiže u decembru. NVIDIA Sync će ovog meseca omogućiti povezivanje do osam DGX Spark sistema u klaster.

ŠTA NEDOSTAJE

NVIDIA ne navodi cene. Pre kupovine proverite da li model koji vam treba staje u memoriju i kolika je brzina pri dužem kontekstu, jer podaci iz objave dolaze od proizvođača.

UKRATKO

RTX Spark

ASUS, Dell, HP, Lenovo, Microsoft i MSI; Acer uskoro

DGX Spark 64 GB

Nemotron 3.5 Bolt 74B, Qwen3.8 27B, Gemma 4 26B

DGX Station

Isporuka u toku; verzija za Windows u decembru

NVIDIA Sync

Klasteri do osam DGX Spark sistema

IZVORI

- 1 **NVIDIA Blog**, Bringing the Spark to Europe: Local Intelligence Powers Next Wave of Agents, 21.10.2026. blogs.nvidia.com

BUILD / PYTORCH CONFERENCE / 20.10.2026.

PyTorch prestaje da bira čip

Google je otvorio TorchTPU, a AWS je pustio TorchNeuron u javnu betu. Isti PyTorch kod sada može da radi na NVIDIA GPU-ovima, Googleovim TPU-ovima i Amazonovim Trainium čipovima, uz male izmene.

JEDAN MODEL, VIŠE AKCELERATORA

GOOGLE

TorchTPU

Open source; vLLM, SGLang, Ray i Hugging Face

AWS

TorchNeuron

Trainium2 i Trainium3; eager i torch.compile; public beta

KUBERNETES

llm-d 1.0

Distribuirana inferencija na GPU i TPU iza jedne adrese

ZAŠTO JE OVO VAŽNO

Većina AI koda piše se u PyTorchu, a PyTorch je godinama najbolje radio na NVIDIA GPU-ovima. Prelazak na drugi akcelerator značio je posebne biblioteke i prepravke. TorchTPU i TorchNeuron koriste zvanične tačke proširenja PyTorch-a, pa se TPU i Trainium ponašaju kao još jedan uređaj. Za firme to znači više izbora i jaču poziciju u pregovorima o ceni računarstva.

ŠTA JE OBJAVLJENO

Google je TorchTPU razvio sa PyTorch timom u Meti, koja ga koristi za jezičke modele, oglase i preporuke. AWS je TorchNeuron pustio kao open source javnu betu za Trainium2 i Trainium3; model se prebacuje jednom linijom koda, ali deo operacija još nije podržan. Deepgram navodi da na Trainiumu obrađuje oko 60% više sekundi zvuka po dolaru. Google, Red Hat i IBM objavili su i llm-d 1.0 za distribuiranu inferenciju na Kubernetesu.

BROJKE PROIZVOĐAČA

Google navodi da je TorchTitan na modelu Qwen 3 8B dostigao do 52% iskorišćenja računarske snage, uz skoro linearno skaliranje do 8.192 Ironwood TPU-a. AWS je rad TorchNeurona proverio na 100.000 modela sa Hugging Facea. Obe brojke dolaze od proizvođača.

BROJKA

8.192

Ironwood TPU-ova u Googleovom testu skaliranja TorchTitana, uz 52% MFU na Qwen 3 8B. [Google Cloud Blog](#)

STATUS

TorchTPU

Open source na GitHubu

TorchNeuron

Public beta, Apache 2.0

llm-d

1.0, CNCF Sandbox

FP8 na Trainiumu

Privatna beta

IZVORI

- 1 **Google Cloud Blog**, TorchTPU is now open source: Run native PyTorch on TPUs, 20.10.2026. cloud.google.com
- 2 **PyTorch**, Introducing TorchNeuron: Native PyTorch backend for AWS Trainium, 20.10.2026. pytorch.org

GitHub zatvara vrata paketima

Posle niza napada preko npm i PyPI paketa, GitHub uvodi firewall koji pakete proverava pre instalacije. Iste nedelje stižu provera licenci, podrška za nove menadžere paketa i gašenje šest Copilot modela.

COPILLOT MODELI UGAŠENI 19. OKTOBRA

UGAŠEN	ZAMENA	NAPOMENA
GPT-5.5 i GPT-5.4	GPT-6.1 Sol	Chat, agent i dovršavanje koda
GPT-5.4 mini, GPT-5 mini	GPT-6 Luna	Zamenu možda uključuje administrator
Gemini 3.7 Flash	Gemini 3.8 Flash	Proveriti automatizacije
Grok 4.5	Grok 4.7	Proveriti automatizacije

PACKAGE FIREWALL

Firewall stoji između vaših računara, CI servera ili agenata i javnih registara. Pre instalacije proverava da li paket ima upozorenje o malveru ili ranjivosti, da li je izgubio potvrdu porekla i da li je stariji od perioda čekanja koji ste zadali. Ako je paket blokiran greškom, izuzetak se traži kroz formular iz poruke o grešci. Posle preview faze naplaćivaće se prema korišćenju.

LICENCE I ZAVISNOSTI

Enterprise Cloud organizacije od 16. oktobra mogu centralno da odrede dozvoljene licence otvorenog koda, a pull request sa nedozvoljenom licencom biva označen. Dependabot sada podržava npm 12, pnpm 11 i 12 i Bun 1.4.

COPILLOT MODELI

Ako vaše automatizacije navode tačan naziv ugašenog modela, izmenite ih.

ZAŠTO SADA

LiteLLM sa strane 15 pokazuje da i zvaničan paket iz zvaničnog registra može biti zlonameran. Period čekanja pre instalacije daje vreme da se takva verzija otkrije i ukloni.

PACKAGE FIREWALL

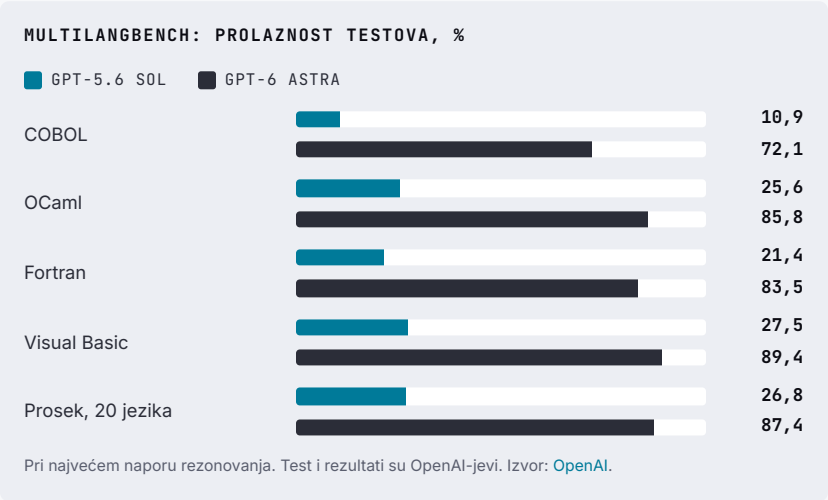
Status
Public preview, besplatno
Za koga
GitHub Enterprise Cloud
Ekosistem
Za sada samo npm

IZVORI

- GitHub Changelog**,
GitHub package firewall in public preview, 20.10.2026.
[github.blog](#)
- GitHub Changelog**,
Open source license compliance generally available, 16.10.2026.
[github.blog](#)
- GitHub Changelog**,
Dependabot now supports npm 12, pnpm 11 and 12, and Bun 1.4, 20.10.2026.
[github.blog](#)
- GitHub Changelog**,
GitHub Copilot models deprecated on October 19, 2026, 19.10.2026.
[github.blog](#)

COBOL više nije prepreka

OpenAI je objavio dva testa za jezike sa malo javnog koda. Najnoviji modeli su na njima skočili sa desetak na 70 do 90 procenata, što menja računicu za održavanje bankarskih i državnih sistema.



DVA TESTA

MultiLangBench traži od modela da od nule napravi bazu kompatibilnu sa SQLiteom, u jednom od 20 jezika. Drugi test prevodi COBOL programe u druge jezike, a migracija važi tek kada skriveni testovi daju bajt po bajt isti izlaz. Tu je GPT-6.1 Sol pri niskom naporu imao 86,6% uspešnih migracija, naspram 5,4% kod GPT-5.6 Sol, uz 39% niži trošak.

ZAMKA

COBOL, koji prema OpenAI-ju pokreće 95% transakcija na bankomatima, odbacuje višak decimala ako zaokruživanje nije traženo. Prepisani program koji zaokružuje radi, ali daje drugačije iznose.

BROJKA

97,9 %

uspešnih COBOL migracija za GPT-6.1 Sol pri višem naporu, u OpenAI testu. [OpenAI](#)

OPREZ

Test je napravio proizvođač modela. Migracija u produkciji i dalje traži sopstvene testove ponašanja, posebno za zaokruživanje novčanih iznosa.

IZVORI

- 1 [OpenAI](#), Advancing coding in low-resource programming languages, 19.10.2026. [openai.com](#)

USE THIS / GITHUB CLI / 21.10.2026.

Tokeni koji sami ističu

GitHub CLI od verzije 2.103.0 može da koristi tokene koji važe nekoliko sati i sami se obnavljaju. Ako takav token procuri iz logova, kao kod LiteLLM-a, napadač dobija sate, a ne neograničeno vreme.

TRI KORAKA

1 / VERZIJA

gh 2.103.0 ili novija
Proverite komandom `gh version`

→

2 / UKLJUČITE

Tokeni sa rokom
`gh config set`
`expiring_credentials`
`enabled`

→

3 / GIT

gh kao pomoćnik
`gh auth setup-git`, uz `git 2.46` ili noviji

Podešavanje važi za prijave posle njega, pa se posle koraka 2 ponovo prijavite komandom `gh auth login`.

ZAŠTO VAM OVO TREBA

Klasičan GitHub CLI token važi dok ga ne opozovete. Ako procuri, napadač ga koristi daniima ili mesecima. Upravo to se dogodilo kod LiteLLM-a: tokeni su završili u logovima, a napadač je sa njima preuzeo proces objavljivanja. Token sa rokom postaje neupotrebljiv za nekoliko sati.

KAKO RADI

Kada uključite opciju, `gh` čuva kratkotrajan token i refresh token koji se redovno menja. Kada token istekne, `gh` ga u pozadini obnovi, pa ne morate ponovo da se prijavljujete. Komanda `gh auth status` pokazuje kada trenutni token ističe.

Za `git` preko HTTPS-a GitHub preporučuje da `gh` bude pomoćnik za kredencijale i `git 2.46` ili noviji. Skripte ne bi trebalo da čuvaju token, nego da ga traže od `gh` svaki put kada im treba.

GDE RADI

Opcija radi na `github.com` i `ghe.com`, a na GitHub Enterprise Serveru od verzije 3.23. Na serverima koji je ne podržavaju `gh` se vraća na tokene bez roka. Postoji i opcija komandne linije za samo jednu prijavu, opisana u GitHub dokumentaciji. GitHub planira da tokeni sa rokom u nekoj budućoj verziji postanu podrazumevani za nove prijave.

KORISNE KOMANDE

Rok tokena

`gh auth status`

Token za skriptu

`gh auth token`

Git preko HTTPS-a

`gh auth setup-git`

ZA SKRIPTE

Ne čuvajte token u fajlu ili promenljivoj. Pozovite `gh auth token` svaki put kada vam treba, jer sačuvan token ističe.

IZVORI

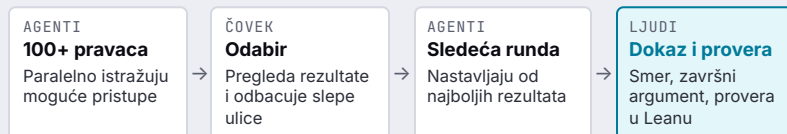
- 1 **GitHub Changelog**,
GitHub CLI: Opt in to
expiring, auto-
refreshing OAuth
tokens, 21.10.2026.
[github.blog](#)

LAB / MICROSOFT RESEARCH / 21.10.2026.

Problem star 31 godinu

Istraživač Microsofta i saradnik dokazali su Kannan-Lovász-Simonovits hipotezu, jedno od važnih otvorenih pitanja visokodimenzionalne geometrije. AI agenti su istražili više od stotinu pravaca, ali su ključni koraci delo ljudi.

KAKO JE NASTAO DOKAZ, PREMA MICROSOFTU



Ponovljeni pokušaji vodećih modela bez ljudskog vođenja, sa sličnim brojem tokena, nisu uspeali, prema Microsoftu.

ŠTA TVRDI HIPOTEZA

KLS hipoteza iz 1995. kaže da je za široku klasu oblika u prostoru sa mnogo dimenzija najbolji ravan rez skoro jednako dobar kao najbolji rez bilo kog oblika, i da razlika ne raste sa brojem dimenzija. Od toga zavisi koliko brzo mogu da rade algoritmi za uzorkovanje i optimizaciju u takvim prostorima.

ULOGA AGENATA

Xinzhi Zhang iz Microsoft Researcha i saradnik koristili su agente koji su paralelno istraživali više od stotinu pravaca. Istraživač je odbacivao neperspektivne i najbolje prosleđivao dalje. Ljudi su izabrali pravac, sastavili završni argument i proverili dokaz. Microsoft navodi da su rekursivni metod, njegova ponovljena primena i dokaz o ograničenju greške originalni doprinos autora.

NEZAVISNA POTVRDA

Istog dana druga grupa objavila je potpun dokaz zasnovan na Microsoftovom radu, a treći dokaz koristi blisku ideju. Deo je formalno proveren u Leanu 4.

RAD

Naslov

An $O(1)$ Bound for the KLS Constant

arXiv

2610.01447, verzije od 01. i 04.10.

Autor

Xinzhi Zhang, Microsoft Research, i saradnik

Provera

Lean 4, deo objavili drugi istraživači

IZVORI

- 1 **Microsoft Research**, Solving a 31-year-old grand challenge in mathematics: the KLS conjecture, 21.10.2026. microsoft.com

LAB / OPENAI, PERTURBAI I SCRIPPS / 20. I 21.10.2026.

Hiljade agenata nad mozgom miša

Hiljade agenata zasnovanih na GPT-Rosalindu analizirale su podatke iz miliona ćelija mišjeg mozga za 32 minuta. Rezultat nisu lekovi, nego istraživački tragovi koje naučnici sada moraju da provere u laboratoriji.

DISTRIBUIRANO BIOLOŠKO ZAKLJUČIVANJE

PODACI

CRISPR atlas mozga

Kako isključeni geni menjaju ćelije

AGENT PO GENU

Hiljade agenata

Svaki analizira jednu promenu i literaturu

SPAJANJE

Atlas zaključivanja

Geni, efekti, radovi i mogući mehanizmi

LJUDI

Eksperiment

Hipoteze se proveravaju u laboratoriji

ŠTA JE URAĐENO

Tim je analizirao postojeći CRISPR atlas mišjeg mozga, koji pokazuje kako isključivanje pojedinačnih gena menja vrste ćelija. Svaki agent je analizirao jednu promenu, pregledao literaturu i predložio objašnjenje, a izveštaji su spojeni u javno dostupan atlas.

Agenti su ponovili nalaze ljudskih analiza i pronašli nove tragove, među njima moguću vezu između regulacije holesterola i neurodegeneracije. Njihove procene poklopile su se sa ocenama stručnjaka koji nisu znali čiju procenu gledaju. To su hipoteze, ne terapije. Tim procenjuje da bi ista analiza, rađena promenu po promenu, ljudima trajala od nekoliko meseci do godinu dana.

ORCHESTRA BIO

Dan ranije OpenAI je kupio Orchestra Bio, platformu u kojoj ljudi i agenti zajedno vode razvoj leka i prate posledice problema, na primer kada neuspela serija u proizvodnji odloži kliničko ispitivanje. OpenAI navodi da razvoj novog leka u SAD u proseku traje 10 do 15 godina.

BROJKA

32 min

za analizu koju bi ljudi, jedan po jedan gen, radili mesecima do godinu dana, prema proceni tima. [OpenAI](#)

ORCHESTRA BIO

Šta je

Platforma za koordinaciju razvoja lekova

Objavljeno

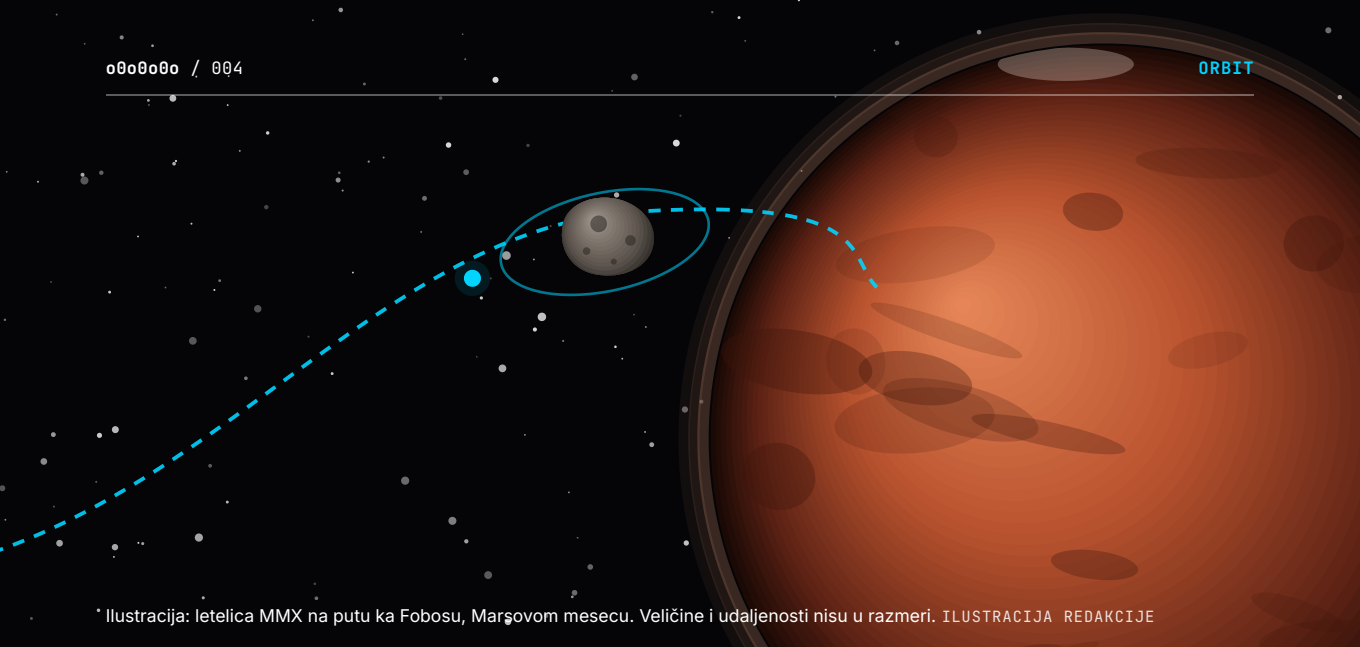
20.10.2026.

Uz

GPT-Rosalind i Rosalind Workbench

IZVORI

- 1 [OpenAI](#), Using thousands of AI agents to uncover new leads in biological data, 21.10.2026. [openai.com](#)
- 2 [OpenAI](#), OpenAI acquires Orchestra Bio, 20.10.2026. [openai.com](#)



* Ilustracija: letelica MMX na putu ka Fobosu, Maršovom mesecu. Veličine i udaljenosti nisu u razmeri. ILUSTRACIJA REDAKCIJE

ORBIT / JAXA / 19. I 20.10.2026.

Deset grama Fobosa

Japanska letelica MMX poletela je na raketi H3 u 21:41 po beogradskom vremenu 19. oktobra. Ako sve prođe po planu, 2031. godine na Zemlju će doneti najmanje deset grama tla sa Marsovog meseca.

LANSIRANJE

Raketa H3 poletela je sa Tanegašime 20. oktobra u 04:41 po japanskom vremenu. Prema JAXA-i, let je protekao po planu, a letelica se odvojila 71 minut posle poletanja.

PLAN

MMX bi u orbitu Marsa trebalo da uđe u avgustu 2027, a mesec dana kasnije u orbitu oko Fobosa. Rover IDEFIX od 25 kilograma, delo francuskog CNES-a i nemačkog DLR-a, biće spušten 2029, a na Fobosu će zbog slabe gravitacije težiti oko 15 grama. Glavna letelica će 2030. dva puta sleteti i uzeti uzorke. ESA daje komunikacione uređaje i zemaljske stanice. Lansiranje je potvrđen uspeh, a sve ostalo su ciljevi misije.

PLAN MISIJE

19.10.2026	Lansiranje, H3 let 10
08.2027.	Orbita oko Marsa
09.2027.	Orbita oko Fobosa
2029.	Rover IDEFIX
2030.	Sletanje i uzorak
2031.	Kapsula u Australiji

IZVORI

- AeroTime**, Japan launches mission to bring back first samples from Mars moon Phobos, 20.10.2026. aerotime.aero
- ESA**, Mars moon lander set to launch on 19 October, 13.10.2026. esa.int
- JAXA**, MMX: Martian Moons eXploration, 2026. mmx.jaxa.jp

FOLLOW UP / 16.10.2026. → 22.10.2026.

Šta se dogodilo od prošlog broja

Teme koje smo u brojevima 002 i 003 najavili ili ostavili otvorenim, i šta se sa njima dogodilo do 22. oktobra.

ORBIT · 16.10.

USSF-481 je poleteo

Falcon 9 je lansiran sa Vandenberg 15. oktobra po pacifičkom vremenu, a prvi stepen je sleteo na platformu u okeanu. U broju 003 ishod još nije bio poznat.

[SpaceX](#)

MODEL · 16.10.

Reflection je objavio Beam

Model koji je u broju 002 bio u najavama sada ima javne težine pod licencom Apache 2.0. Detalji na strani 18.

[Reflection AI](#)

AGENTI · 20.10.

Nenamerne radnje, drugi put

Posle Anthropicovog izveštaja iz broja 003, sada i OpenAI opisuje agente koji su oslabili sopstveni nadzor. Strana 08.

[Reuters](#)

APPLE · 16.10.

Počela pretprodaja iPhone Duo

Appleov telefon na preklap može da se naruči u SAD i delu drugih zemalja. Rokovi isporuke su odmah počeli da se produžavaju.

[MacRumors](#)

ANTHROPIC · 20.10.

Prospekt pred berzu

Nacrtr prospekta pokazuje neto gubitak od 80,7 mlrd \$ za prvu polovinu godine, uglavnom zbog računovodstvenog troška. Izlazak na berzu se očekuje sredinom novembra. Strana 23.

[Reuters](#)

ARTEX · 21.10.

Alat iz broja 002 u novom napadu

U broju 002 pisali smo o alatu ARTEX posle napada na korejsku banku. Microsoft sada navodi da ga je Storm-0940 koristio protiv ConnectWisea. Strana 07.

[Microsoft Security](#)

SHIPPED / 16.10.2026. → 22.10.2026.

Stiglo ove nedelje

Samo ono što je zaista postalo dostupno, sa statusom iz zvaničnog izvora.

MODEL · 19.10.

Mercury 3

Difuzioni model preko Inception API-ja, OpenRoutera, Basetena i Vercela, sa kontekstom od milion tokena.

DOSTUPNO Inception

GLAS · 20.10.

Voxtral 3

Modeli za prepoznavanje i sintezu govora i SDK za glasovne agente, preko Mistralovog API-ja.

DOSTUPNO Mistral AI

CLOUDFLARE · 21.10.

WAF koji vidi i odgovor

Full transaction detection za sve zone, i na besplatnom planu, uz do tri pravila za odgovor.

GA Cloudflare

GITHUB · 20.10.

Package Firewall

Provera npm paketa pre instalacije na CI hostovima i za agente. Enterprise Cloud.

PUBLIC PREVIEW GitHub ChangeLog

AWS · 20.10.

TorchNeuron

Izvorni PyTorch backend za Trainium2 i Trainium3, open source.

BETA PyTorch

MODEL · 16.10.

Beam, otvorene težine

501 milijarda parametara na Hugging Faceu, pod licencom Apache 2.0.

DOSTUPNO Reflection AI

API · 17.10.

DeepSeek Search i Fetch API

Pretraga i preuzimanje stranica za agente, 0,75 \$ na 1.000 poziva.

GA DeepSeek API Docs

GITHUB · 16.10.

Provera licenci zavisnosti

Pravila o dozvoljenim licencama za Enterprise Cloud, uz GitHub Code Security.

GA GitHub ChangeLog

GITHUB · 21.10.

Tokeni koji ističu u gh

Opcija od verzije 2.103.0. Uputstvo na strani 30.

PUBLIC PREVIEW GitHub ChangeLog

ANTHROPIC · 21.10.

Claude Security, stalno skeniranje

Praćenje ispravki, API i MCP konektor. Za Claude Enterprise korisnike.

BETA Claude

NAJAVLJENO, JOŠ NIJE DOSTUPNO

Claude Duet lista čekanja, samo SAD
OpenAI na Google Cloudu GA u narednim nedeljama
Google A5X GA sledećeg meseca

DGX Spark 64 GB od 23.10.
OpenShell arhitektura bez roka
MiniMax težine kasnije

5 MINUTES / 16.10.2026. → 22.10.2026.

Ukratko

Osam vesti koje nisu dobile posebnu stranu, a vredi ih znati.

DEVELOPERI · 20.10.

TypeScript prepisan u Rust

Cloudflare i VoidZero objavili su eksperimentalni tsrs, port TypeScript kompajlera u Rust. Prema autorima, do osam puta je brži od TypeScripta 7.0 i troši oko 70% manje memorije.

[Cloudflare](#)

PHP · 21.10.

PHP 8.6 RC4

Četvrti kandidat za PHP 8.6 sadrži ispravke za PHP2Shell, ali nije za produkciju. RC5 je planiran za 5. novembar.

[PHP](#)

DATA CENTRI · 21.10.

Data centar za dve nedelje

NVIDIA je pokazala DSX POD, fabrički sklopljene module sa Vera Rubin platformom. Postavljaju se za oko dve nedelje umesto šest meseci, prema kompaniji.

[Reuters](#)

META · 21.10.

Kazna od 25 mlrd \$

Sudija u Novom Meksiku izrekao je kaznu posle odluke porote da je Meta obmanjivala stanovnike države o deljenju podataka, u slučaju vezanom za Cambridge Analyticu.

[Reuters](#)

CLOUDFLARE · 19.10.

Clairic izvlači podatke

Model koji iz nestrukturiranog teksta izvlači i procenjuje vrednosti, a naplaćuje samo ulazne tokene. Preview na Workers AI, otvorene težine najavljene.

[Cloudflare](#)

ROBOTI · 21.10.

Do 2.000 humanoida

Nemački Agile Robots planira da sledeće godine uz NVIDIA-u proizvede 1.000 do 2.000 malih humanoidnih robota, rekao je direktor kompanije Reutersu.

[Reuters](#)

ANTHROPIC · 18.10.

5% akcija za javno dobro

Predloženi fond bi dobijao još 2% akcija za svakih 50% rasta vrednosti iznad neobjavljene osnovice, po odluci upravnog odbora.

[Reuters](#)

ORBIT · 20.10.

Bandwagon-5

SpaceX je sa Floride lansirao misiju Bandwagon-5, uz sletanje prvog stepena na platformu u okeanu.

[SpaceX](#)

THIS WEEK IN NUMBERS / 16.10.2026. → 22.10.2026.

Nedelja u brojkama

9,2_{cvss}

ocena obe PHP2Shell ranjivosti, po verziji 4 skale

PHP · 21.10.

1,5_{mil.}

hostova sa verzijom PHP-a bez ispravke, od 2,6 miliona, prema Censysu

REUTERS · 21.10.

1.200+

pokušaja upada agenata jednog operatera u Cairnu, više od 100 uspešnih

REUTERS · 19.10.

2.250+

Microsoft 365 tenanata sa pokušajima prijave u kampanji protiv ConnectWisea

MICROSOFT SECURITY · 21.10.

8_{CA}

eMudhra posredničkih sertifikata sa slabim ključevima, šest za TLS

MOZILLA BUGZILLA · 17.10.

1.295

novih bezbednosnih zakrpa u Oracleovom oktobarskom paketu

ORACLE · 20.10.

1.068_{tok/s}

Mercury 3 na NVIDIA GPU-ovima, prema Inceptionu

INCEPTION · 19.10.

501_{mlrd}

parametara modela Beam, 23 milijarde aktivnih, licenca Apache 2.0

REFLECTION AI · 16.10.

72_{mlrd \$}

računovodstveni trošak u Anthropicovom neto gubitku od 80,7 mlrd \$

REUTERS · 20.10.

89

zemalja sa oglasima u ChatGPT-u, među njima i Srbija

OPENAI · 21.10.

32_{min}

za analizu podataka iz miliona ćelija mozga miša, uz hiljade agenata

OPENAI · 21.10.

10_g

najmanja količina tla sa Fobosa koju MMX treba da vrati 2031.

ESA · 19.10.

NEXT / 16.10.2026. → 22.10.2026.

Šta pratimo

Zakazani događaji i teme koje se razvijaju. Ništa od ovoga nije predviđanje.

→ 23.10.

DGX Spark 64 GB

Konfiguracija sa 64 GB stiže kod NVIDIA-inih partnera.

[NVIDIA Blog](#)

→ 27.10.

LiteLLM, ranjivost pod embargom

Enterprise korisnici već imaju ispravku. Javna objava je najavljena za 27. oktobar.

[LiteLLM](#)

→ 05.11.

PHP 8.6 RC5

Peti kandidat za izdanje PHP 8.6.

[PHP](#)

→ 17. DO 20.11.

Microsoft Ignite

Prilika da Microsoft objavi rokove za kontrole agenata sa strane O8.

[Microsoft Security](#)

→ 31.12.

Kraj podrške za PHP 8.2

Posle tog datuma grana 8.2 ne dobija ni bezbednosne ispravke.

[PHP](#)

→ 27.10.

Chrome uklanja emSign koren

Sajtovi sa sertifikatima ispod emSign ECC Root CA G3 do tada treba da pređu na drugu hijerarhiju.

[Google](#)

→ 31.10.

DeepSeek naplaćuje pretragu

Pozivi Search API-ja iz alata u DeepSeek Harnessu, Claude Codeu i Codexu naplaćuju se od 16:00 UTC.

[DeepSeek API Docs](#)

→ SREDINA NOVEMBRA

Anthropic na berzi

Očekivano prvo javno trgovanje akcijama. OpenAI do tada pokušava da zaključi svoju rundu.

[Reuters](#)

→ NAREDNIH NEDELJA

OpenAI na Google Cloudu

Opšta dostupnost modela u Model Gardenu.

[OpenAI](#)

→ 08.2027.

MMX stiže do Marsa

Ulazak u orbitu Marsa, a mesec dana kasnije i oko Fobosa.

[ESA](#)

IZVORI / 16.10.2026. → 22.10.2026.

Svi izvori broja

Izvori po stranama na kojima se prvi put pojavljuju. Primarni izvori imaju prednost.

06 SIGNAL: HAKER KOJI JE SKORO SVE PREPUSTIO AGENTIMA

1. **Reuters.** How one hacker used AI agents and a few thousand dollars to break into scores of sites. 19.10.2026.
[reuters.com/legal/government/how-one-hacker-used-...](#)
2. **NorForge.** Inside Cairn: Open Windows into massive AI-Driven Cyber Operations. 19.10.2026.
[norforge.com/blog/inside_cairn](#)

07 SIGNAL: STORM-0940 I CONNECTWISE

3. **Reuters.** Chinese-linked hackers compromise ConnectWise, target hundreds in global attack, Microsoft says. 21.10.2026.
[reuters.com/technology/chinese-linked-hackers-com...](#)
4. **Microsoft Security.** AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise. 21.10.2026.
[microsoft.com/en-us/security/blog/2026/10/21/stor...](#)

08 SIGNAL: AGENT JE NOVI INSAJDER

5. **Microsoft Security.** Agents are your newest insiders: security must move at their speed. 19.10.2026.
[microsoft.com/en-us/security/blog/2026/10/19/agen...](#)
6. **Reuters.** OpenAI says its AI agents weakened internal monitoring system. 20.10.2026.
[reuters.com/legal/litigation/openai-says-its-ai-a...](#)

09 SIGNAL: ODBRANA UČI DA RADI ISTOM BRZINOM

7. **OpenAI.** Patch the Planet: global response coordination as agents uncover critical vulnerabilities. 21.10.2026.
[openai.com/index/coordinated-disclosure-of-critic...](#)
8. **Claude.** Claude Security now scans continuously and tracks fixes. 21.10.2026.
[claude.com/resources/articles/claude-security-now...](#)
9. **Cloudflare.** Introducing full transaction detection for Cloudflare WAF. 21.10.2026.
[blog.cloudflare.com/full-transaction-waf/](#)

11 PHP2SHELL: ŠTA JE TAČNO POGOĐENO

10. **PHP.** PHP 8.5.12, 8.4.27, 8.3.36 i 8.2.35, kritične bezbednosne ispravke. 21.10.2026.
[php.net/](#)
11. **php-src na GitHubu.** GHSA-w8hw-w9fx-j79w, CVE-2026-109618. 21.10.2026.
[github.com/php/php-src/security/advisories/GHSA-w...](#)
12. **Wiz.** PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the internet. 21.10.2026.
[wiz.io/blog/php2shell-php-rce](#)
13. **Reuters.** Government websites go dark after AI-discovered flaw sparks security scramble. 21.10.2026.
[reuters.com/world/asia-pacific/eu-agency-warns-we...](#)

12 PHP2SHELL: OD HILJADA DO MILIONA

14. **Reuters.** Cloudflare sees millions of exploit attempts after PHP disclosure. 22.10.2026.
[reuters.com/world/asia-pacific/cloudflare-sees-mi...](#)

15. **Reuters.** PHP developers issue updates to fix vulnerabilities, says flaw was found in 2024. 21.10.2026.
[reuters.com/business/php-programming-language-dev...](#)

13 PHP2SHELL: ŠTA DA URADITE DANAS

16. **Cloudflare.** Cloudflare deploys protections against php2shell vulnerability. 21.10.2026.
[blog.cloudflare.com/php-vulnerabilities-waf-prote...](#)

14 PATCH NOW: ZAKRPITI ODMAH

17. **LiteLLM.** Contained: Oct 21, 2026 LiteLLM release v1.107.0 Compromised. 21.10.2026.
[docs.litellm.ai/blog/security-incident-oct-21-2026](#)
18. **Google.** Protecting Chrome and Android Users from Compromised eMudhra Intermediate CA Certificates. 20.10.2026.
[blog.google/security/protecting-chrome-and-androi...](#)
19. **Mozilla Bugzilla.** Bug 2083449, eMudhra: Private key compromise of Intermediate Certificates. 17.10.2026.
[bugzilla.mozilla.org/show_bug.cgi?id=2083449](#)
20. **Oracle.** Oracle Critical Patch Update Advisory, October 2026. 20.10.2026.
[oracle.com/security-alerts/cpuoct2026.html](#)

16 SECURITY: RAILWAY I OPENCODE

21. **Railway.** Security Disclosure: Wednesday October 21st. 21.10.2026.
[blog.railway.com/p/security-disclosure-wednesday-...](#)
22. **Railway.** Security Disclosure Recommendation: Check for anomalous GitHub access. 22.10.2026.
[blog.railway.com/p/security-disclosure-recommenda...](#)
23. **OpenCode na X-u.** Obaveštenje o probouju u Console sistemu. 17.10.2026.
[x.com/opencode/status/2111519637049319818](#)
24. **Cyera.** OpenCode Breach: What Happened and How to Rotate Exposed AI API Keys. 17.10.2026.
[cyera.com/research/opencode-breach-what-happened-...](#)

17 SECURITY: EMUDHRA I HTTPS

25. **Cloudflare.** 8 eMudhra certificates are compromised. 20.10.2026.
[blog.cloudflare.com/emudhra-certificate-compromis...](#)

18 MODEL WATCH

26. **Inception.** Diffusion at Scale: Introducing Mercury 3. 19.10.2026.
[inceptionlabs.ai/blog/introducing-mercury-3](#)
27. **MiniMax.** MiniMax M3.1 Flash: Redefining Agent Performance and Cost. 19.10.2026.
[minimax.io/blog/minimax-m31f](#)
28. **Reflection AI.** Beam is now available. 16.10.2026.
[reflection.ai/blog/beam-is-available](#)
29. **DeepSeek API Docs.** DeepSeek-V4.1-Flash-1017 i Search API. 17.10.2026.
[api-docs.deepseek.com/news/news261017](#)

19 PRIČA: MISTRAL VOXTRAL 3

30. **Mistral AI.** Voxtral 3. 20.10.2026.
[mistral.ai/news/voxtral-3/](#)

IZVORI / NASTAVAK

20 PRIČA: CLAUDE DUET

31. **Claude.** Introducing Claude Duet. 21.10.2026.
claude.com/resources/articles/claude-duet

21 PLATFORME: CHATGPT OGLASI U SRBIJI

32. **OpenAI.** ChatGPT Ads expands to 26 new countries as over 100,000 advertisers have used the platform. 21.10.2026.
openai.com/index/chatgpt-ads-expands-26-new-count...
33. **OpenAI.** OpenAI models are coming to Google Cloud. 21.10.2026.
openai.com/index/openai-models-google-cloud/

22 MONEY: META MUSE

34. **Reuters.** Meta puts Muse agent at heart of AI strategy, plans new stock to power investments. 21.10.2026.
reuters.com/business/meta-issue-new-class-shares-...

23 MONEY: KO PLAĆA AI TRKU

35. **Reuters.** Anthropic logged net loss of over \$80 billion in first half of 2026. 20.10.2026.
reuters.com/business/anthropic-recorded-net-loss-...
36. **Reuters.** OpenAI seeks to accelerate fundraising ahead of Anthropic IPO, sources say. 19.10.2026.
reuters.com/world/openai-seeks-accelerate-fundrai...
37. **Reuters.** DeepSeek wrapping up \$15 billion fundraising to fuel AI race. 22.10.2026.
reuters.com/world/asia-pacific/deepseek-raises-15...

24 MONEY: NVIDIA KAO CENTRALNA BANKA

38. **Reuters Breakingviews.** Nvidia emerges as the central bank of AI. 20.10.2026.
reuters.com/commentary/breakingviews/nvidia-emerg...

25 INFRA: GTC BERLIN

39. **NVIDIA Blog.** Google Cloud and NVIDIA Announce General Availability of NVIDIA Vera Rubin Infrastructure. 21.10.2026.
blogs.nvidia.com/blog/google-cloud-vera-rubin-inf...
40. **Reuters.** Nvidia's Huang hails Europe's AI potential, flanked by robot ducks. 21.10.2026.
reuters.com/business/germanys-agile-make-up-2000-...
41. **NVIDIA Blog.** NVIDIA Cloud Partners Scale Across Europe: Sovereign, Open and Built for Safe AI Agents. 21.10.2026.
blogs.nvidia.com/blog/cloud-partners-europe-sover...

26 INFRA: LOKALNI AI

42. **NVIDIA Blog.** Bringing the Spark to Europe: Local Intelligence Powers Next Wave of Agents. 21.10.2026.
blogs.nvidia.com/blog/local-ai-gtc-rtx-dgx-spark-...

27 BUILD: PYTORCH NA SVIM ČIPOVIMA

43. **Google Cloud Blog.** TorchTPU is now open source: Run native PyTorch on TPUs. 20.10.2026.
cloud.google.com/blog/topics/ai-infrastructure/to...
44. **PyTorch.** Introducing TorchNeuron: Native PyTorch backend for AWS Trainium. 20.10.2026.
pytorch.org/blog/introducing-torchneuron-native-p-...

28 BUILD: GITHUB ZATVARA VRATA PAKETIMA

45. **GitHub Changelog.** GitHub package firewall in public preview. 20.10.2026.
github.blog/changelog/2026-10-20-github-package-f-...

46. **GitHub Changelog.** Open source license compliance generally available. 16.10.2026.
github.blog/changelog/2026-10-16-open-source-lice...
47. **GitHub Changelog.** Dependabot now supports npm 12, pnpm 11 and 12, and Bun 1.4. 20.10.2026.
github.blog/changelog/2026-10-20-dependabot-now-s...
48. **GitHub Changelog.** GitHub Copilot models deprecated on October 19, 2026. 19.10.2026.
github.blog/changelog/2026-10-19-github-copilot-m...

29 BUILD: COBOL VIŠE NIJE PREPREKA

49. **OpenAI.** Advancing coding in low-resource programming languages. 19.10.2026.
openai.com/index/low-resource-programming-languag...

30 USE THIS: TOKENI KOJI SAMI ISTIČU

50. **GitHub Changelog.** GitHub CLI: Opt in to expiring, auto-refreshing OAuth tokens. 21.10.2026.
github.blog/changelog/2026-10-21-github-cli-opt-i...

31 LAB: KLS HIPOTEZA

51. **Microsoft Research.** Solving a 31-year-old grand challenge in mathematics: the KLS conjecture. 21.10.2026.
microsoft.com/en-us/research/blog/solving-a-31-ye...

32 LAB: HILJADE AGENATA U BIOLOGIJI

52. **OpenAI.** Using thousands of AI agents to uncover new leads in biological data. 21.10.2026.
openai.com/index/scaling-ai-research-for-complex-...
53. **OpenAI.** OpenAI acquires Orchestra Bio. 20.10.2026.
openai.com/index/openai-to-acquire-orchestra-bio/

33 ORBIT: MMX KA FOBOSU

54. **AeroTime.** Japan launches mission to bring back first samples from Mars moon Phobos. 20.10.2026.
aerotime.aero/articles/japan-mmx-phobos-sample-re...
55. **ESA.** Mars moon lander set to launch on 19 October. 13.10.2026.
esa.int/Science_Exploration/Space_Science/Mars_mo...
56. **JAXA.** MMX: Martian Moons eXploration. 2026.
mmx.jaxa.jp/en/

34 FOLLOW UP: OD PROŠLOG BROJA

57. **SpaceX.** Launches. 22.10.2026.
spacex.com/launches
58. **MacRumors.** iPhone Duo Now Available to Pre-Order From Apple. 16.10.2026.
macrumors.com/2026/10/16/iphone-duo-now-available...

36 5 MINUTES

59. **Cloudflare.** Introducing tsrs: A port of TypeScript to Rust. 20.10.2026.
blog.cloudflare.com/typescript-rust-port/
60. **Cloudflare.** Introducing Clairic, a new System One class of extraction models. 19.10.2026.
blog.cloudflare.com/clairic-extraction-model/
61. **Reuters.** Anthropic's public benefit fund and how it compares with other big philanthropic efforts. 20.10.2026.
reuters.com/business/anthropics-public-benefit-fu...

o0o0o0o0

/ 004

Nedeljni pregled tehnologije. Besplatno,
na tutorijali.app.

Izdanje 004

Datum 22.10.2026.

Period 16.10.2026. 08:00 → 22.10.2026. 10:00

Web tutorijali.app



tutorijali.app