oOoOoOo / 006

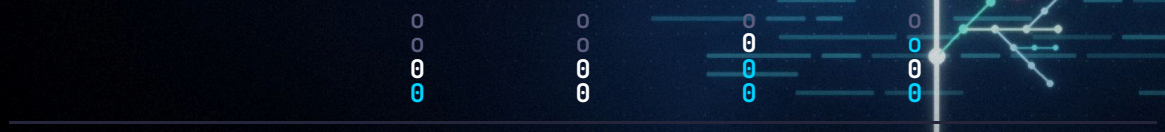
06.11.2026.
NEDELJNI PREGLED TEHNOLOGIJE
TUTORIJALI.APP

TEMA BROJA

BITKA ZA KOD

AI više ne piše samo softver. Pronalazi ranjivosti, razvija zakrpe i menja infrastrukturu na kojoj nastaje sledeća generacija aplikacija.

08 GPT-6 CYBER 948 Linux ranjivosti, 81 Firefox otkriće
16 PANDO, PIERRE, CONDUCTOR Nova borba za alate
26 IMAGES 2.6 GIF, SVG i brže uređivanje slika
28 GOOGLE MEET Govorno prevođenje na 63 jezika
33 ANDROID GHOSTMAP Telefon može ostati u petlji rušenja
42 FLASHPROVE Kriptografski dokaz AI odgovora
49 AMD Rekordan rast AI Data Center poslovanja
57 ORBIT Kraj misije Swift posle skoro 22 godine



0 velika priča o vest 0 agenti

Jedan znak, jedan događaj

31.10.2026. 00:00 → 05.11.2026. 22:15, Beograd

Besplatno izdanje u PDF formatu

Sadržaj

Broj je podeljen po rubrikama, a svaka rubrika ima svoju boju. Brojevi strana su linkovi.

04 UVODNIK
Skupo je sve posle koda

05 TEMA BROJA
Bitka za kod
Pet frontova oko jednog pitanja.

06 TEMA BROJA
Kod je postao infrastruktura

07 TEMA BROJA
Kontrola je postala glavni trošak

08 SECURITY
AI je ušao u novu fazu sajberbezbednosti
GPT-6 Cyber, Critical i ograničen pristup.

09 SECURITY
Šta testovi pokazuju, a šta ne

10 SECURITY
948 puteva do root pristupa

11 SECURITY
Od kandidata do zakrpe

12 SECURITY
Šta 948 ne znači

13 SECURITY
Firefox: 81 nova ranjivost

14 SECURITY
Ko sme da drži najjači model

15 BUILD
Kod više nije usko grlo. Infrastruktura jeste.

16 BUILD
Git koji je napravljen za agente
Zašto je OpenAI promenio ono što je iza Gita.

17 BUILD
Tri odluke iza Panda

18 BUILD
OpenAI kupuje sloj za pregled koda

19 BUILD
Conductor prelazi u Metu

20 BUILD
Četiri sloja, četiri vrste proizvoda

21 BUILD
Copilot u Xcodeu, BYOK i veštine agenata

22 BUILD
Ko dobija poruku kada procuri ključ

23 BUILD
Svaki push prolazi kroz AI pregled

24 BUILD
Better Auth: 12 upozorenja odjednom

25 BUILD
Sitne promene na Vercelu

26 MODEL WATCH
Images 2.6: slike dobijaju pokret
GIF, SVG i preciznije uređivanje.

27 MODEL WATCH
Flare ili Sunburst

28 MODEL WATCH
Google Meet ruši jezičke barijere
63 jezika i automatsko prepoznavanje.

29 MODEL WATCH
Ko može da ga koristi i šta može da krene naopako

30 MODEL WATCH
Muse dobija glas i lice

31 MODEL WATCH
Modeli nedelje

32 MODEL WATCH
Od skice do aplikacije, od testa do života

33 SECURITY SIGNAL
GhostMap: aplikacija bez koda koja ruši telefon
Rušenje bez pokretanja aplikacije.

34 SECURITY SIGNAL
Kada se dva parsera ne slože

35 PATCH NOW
Zakrpiti odmah

36 SECURITY SIGNAL
Kada sajbernapad promeni temperaturu u frižideru

37 SECURITY SIGNAL
Alarm koji ne zavisi od napadnutog sistema

38 SECURITY SIGNAL
Zyxel: tri izvora, tri različite stvari

39 SECURITY SIGNAL
Kada je pouzdan izvor problem

40 SECURITY SIGNAL
Plaćati ljude da nađu ono što modeli propuste

41 SECURITY SIGNAL
Kratki bezbednosni pregled

42 LAB
Može li se matematički dokazati da je AI zaista radio ono što tvrdi?
Zero-knowledge dokaz za odgovor modela.

43 LAB
Dokaz o poreklu nije dokaz o istini

44 LAB
Claude i misterija šupljih čestica

45 LAB
Za šta naučnici zaista koriste Claude

46 LAB
Do 15 puta brže, u jednom zamišljenom svetu

47 LAB
Sat vremena hemije, ne sat do leka

48 LAB
Od CAD modela do stvarnog dela

49 MONEY
AMD: Data Center skoro duplo veći
Rekordan kvartal i Data Center.

50 MONEY
AMD u četiri grafikona

51 MONEY
Apple: rekord bez AI priče u brojkama

52 MONEY
Arm prodaje nacrte, a sada i više od toga

53 INFRA
Kako izgleda garancija od 401 megavat

54 INFRA
Računarski kampus kao rezerva za mrežu

55 MONEY
Ko zarađuje u ovoj fazi

56 WORK
Kako uključiti prevođenje u Google Meetu

57 ORBIT
Swift je završio misiju
Kraj misije posle skoro 22 godine.

58 ORBIT
Dvadeset dve godine u jednoj liniji

59 ORBIT
X-70 Fractal: avion koji menja opremu

60 ORBIT
Dva preleta, jedna fotografija, jedno sletanje

61 USE THIS
Proverite svoje workflowe pre 9. novembra

62 USE THIS
Ne ukidajte zaštitu zbog jednog workflowa

63 SHIPPED
Stiglo ove nedelje

64 5 MINUTES
Ukratko

65 BROJKE
Nedelja u brojkama

66 BROJKE
Još brojki nedelje

67 NEXT
Šta pratimo

68 IZVORI
Svi izvori broja

UVODNIK / BROJ 006

Skupo je sve posle koda

Šesti broj izlazi u petak, 6. novembra, posle nedelje u kojoj je kod prestao da bude najteži deo softvera.

Prošli broj pitao je ko kontroliše AI. Ovaj počinje jednu stepenicu niže, tamo gde se kontrola zaista sprovodi: u kodu.

Za samo šest dana OpenAI je pokazao sistem koji za jedan prolaz kroz Linux jezgro proizvede 948 radnih exploita, predstavio Git backend napravljen zato što stari više nije stizao da prati agente i najavio kupovinu kompanije koja pravi alate za pregled izmena. Meta je kupila Conductor, GitHub menja podrazumevana pravila za Actions, Vercel uvodi automatski bezbednosni pregled svakog pusha, a Anthropic objavljuje kriptografski dokaz da je odgovor zaista dao model koji je naveden.

Sve to izgleda kao šest različitih vesti, ali opisuje isto pomeranje. Pisanje koda više nije najskuplji deo posla. Skupe su provera, integracija, pregled, zakrpa i poverenje u rezultat. Tu se sada vodi bitka.

Zato prema brojkama iz ovog broja treba biti pažljiv. Većina potiče od samih proizvođača, a 948 exploita nije isto što i 948 zakrpa. Razliku između tvrdnje, potvrde i plana vodimo na svakoj strani.

Broj zatvaramo u četvrtak, 5. novembra, u 22:15. Dobro čitanje.

O IZDANJU

Broj
006

Izdanje
06.11.

Presek
05.11. u 22:15

Period
31.10. do 05.11.

Glavna tema
Bitka za kod

KAKO ČITATI BROJKE

Benchmarkovi i rezultati istraživanja koje objavljuju proizvođači označeni su kao njihove tvrdnje. Procene i planovi nisu potvrđene činjenice.

TEMA BROJA / PET FRONTOVA

Bitka za kod

Šta se događa kada AI pronalazi stotine ranjivosti, a isti talas menja alate na kojima softver nastaje? Pet pitanja vodi kroz ceo broj.



1 RANJIVOSTI
Šta se dešava kada AI nalazi stotine grešaka i predlaže zakrpe? 08
GPT-6 Cyber, Linux, Firefox.

2 INFRASTRUKTURA
Zašto OpenAI i Meta ulažu u paralelno programiranje? 16
Pando, Pierre, Conductor.

3 POVERENJE
Možemo li dokazati da je odgovor dao deklarisani model? 42
FlashProve i cena dokaza.

4 SVAKODNEVICA
Kako slike, glas i prevod menjaju svakodnevnu upotrebu AI-ja? 26
Images 2.6, Google Meet, Muse.

5 NOVAC
Kako se sve to vidi u čipovima, energiji i ugovorima? 49
AMD, Arm, TeraWulf, Grid Protectors.

Pisanje koda više nije najskuplji deo posla. Skupi su provera, integracija, zakrpa i poverenje u rezultat.

TEMA BROJA / ANALIZA / 06.11.2026.

Kod je postao infrastruktura

Agenti su ubrzali jednu fazu razvoja softvera. Sve ostale sada moraju da ih stignu.

Kada programer napiše funkciju, ona je tek početak posla. Neko mora da je pregleda, spoji sa tuđim izmenama, testira, objavi i kasnije zakrpi. Dok je kod pisao čovek, sve te faze imale su približno isti tempo. Agenti su taj odnos pokvarili.

Anthropic je u oktobru objavio da je u maju spajao oko 2.500 izmena dnevno, a u septembru više od 30.000. OpenAI opisuje isti pritisak: krajem prošle godine pouzdanost njegovog monorepozitorijuma povremeno je padala ispod 90%. Obe kompanije su rešile problem na isti način, pravljenjem sopstvene infrastrukture.

Isti obrazac važi u bezbednosti. Pronalaženje greške je sve jeftinije, pa usko grlo postaje ono što dolazi posle. OpenAI to kaže otvoreno: prioritizacija i validacija ostaju operativno ograničenje, a ne otkrivanje.

ČETIRI FRONTA ISTE BITKE

Na prvom frontu su ranjivosti, gde modeli traže greške brže nego što ih ljudi mogu pregledati. Na drugom je sam Git i sve oko njega. Na trećem je poverenje: možemo li uopšte dokazati šta je model uradio. Četvrti je novac, jer sve ovo traži čipove, struju i ugovore na decenije.

Kod je postao infrastruktura. Ko kontroliše tu infrastrukturu, kontroliše i tempo svega ostalog.

BROJKA

12 puta

rast dnevnih spajanja koda u Anthropicu, od oko 2.500 u maju do više od 30.000 u septembru. Anthropic

BROJKA

< 90 %

pouzdanost OpenAI monorepozitorijuma u najgorim trenucima pre Panda. OpenAI

IZVORI

1 **Anthropic**, Redesigning source control at Anthropic, 13.10.2026. anthropic.com

2 **OpenAI**, Scaling Git at OpenAI, 02.11.2026. openai.com

3 **OpenAI**, A thousand fewer paths to root, 04.11.2026. openai.com

TEMA BROJA / ANALIZA / 06.11.2026.

Kontrola je postala glavni trošak

PET FRONTOVA OVE NEDELJE

RANJIVOSTI	**Provera nalaza** 2.308 kandidata, 1.724 potvrđene, 948 exploita, 1,2 miliona dolara	10
GIT	**Nova infrastruktura** Pando i Scion nastali su zato što stari sistemi nisu stizali	16
PRAVILA	**Podrazumevana zaštita** pull_request_target se blokira od 2. decembra	61
POVERENJE	**Dokaz izvršavanja** 70 do 95 puta više GPU vremena po zahtevu	42
NOVAC	**Kapacitet** AMD Data Center +97%, 401 MW za Anthropic, 1.000 MW fleksibilnosti	49

Sve brojke su iz izvora navedenih na stranama članaka.

Ove nedelje najčešći trošak nije bio novi model, nego kontrola oko njega. OpenAI uz GPT-6 Cyber traži proveru identiteta, jednokratnu prijavu, višefaktorsku autentifikaciju i spisak dozvoljenih IP adresa. GitHub menja podrazumevanu vrednost za okidač koji je godinama bio izvor problema. Vercel svaki push šalje na AI pregled, ali izričito piše da to nije bezbednosna revizija.

Ista logika važi i za istraživanje. Anthropicov prototip dokazuje da je odgovor dao određeni model, po ceni od oko 70 do 95 puta više GPU vremena. To je skup odgovor na pitanje koje do sada nije imalo nikakav odgovor.

Otvoreno ostaje ko će plaćati ovu dodatnu proveru. Održavaoci Linuxa već primaju stotine prijava. Mali timovi moraće da pregledaju svoje workflowe do 2. decembra, a korisnici mSecurea menjaju svaku lozinku bez objašnjenja zašto.

IZVORI

1 **OpenAI**, A thousand fewer paths to root, 04.11.2026. openai.com

2 **OpenAI**, GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents, 05.11.2026. openai.com

3 **Anthropic**, Provable inference and FlashProve, 02.11.2026. anthropic.com



COVER STORY / OPENAI / 05.11.2026.

AI je ušao u novu fazu sajberbezbednosti

GPT-6 Cyber je prvi OpenAI sajber model koji se, po proceni same kompanije, svrstava u kategoriju Critical. Dostupan je samo odobrenim korisnicima.

OpenAI je 5. novembra predstavio GPT-6 Cyber, varijantu modela GPT-6 Astra koja je dodatno trenirana za autorizovano istraživanje ranjivosti. Model nije opšte dostupan. U prvoj fazi dobija ga izabrana grupa odobrenih korisnika programa Daybreak Red, preko API-ja i Codexa.

Kompanija ga po svom okviru Preparedness Framework svrstava u kategoriju Critical za sajberbezbednost, dok je prethodni GPT-5.6 Cyber bio High. Ista oznaka važi i za GPT-6 Astra, pa ovo nije izuzetak nego novi nivo modela u celini.

Na testu ExploitGym, koji meri da li model može da iskoristi zadatu ranjivost na udaljenoj meti, GPT-6 Cyber postiže 48,5%, naspram 32,1% za prethodnika. To je oko 16 procentnih poena, odnosno 51% relativno. Sve brojke u ovom tekstu su rezultati koje je objavio proizvođač i nisu nezavisno potvrđene.

Važnije od same brojke je ono što OpenAI navodi kao rezultat u stvarnom softveru: 81 prethodno nepoznata ranjivost visoke ozbiljnosti u Firefoxu i 948 radnih exploita za lokalnu eskalaciju privilegija u Linuxu. Time se bave sledeće strane.

BROJKA

48,5 %

ExploitGym, rezultat koji navodi OpenAI. OpenAI

STATUS

Tip
Specijalizovan model

Osnova
GPT-6 Astra

Pristup
Daybreak Red

Kanali
API, Codex

Sajber oznaka
Critical

IZVORI

1 **OpenAI**, GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents, 05.11.2026. openai.com

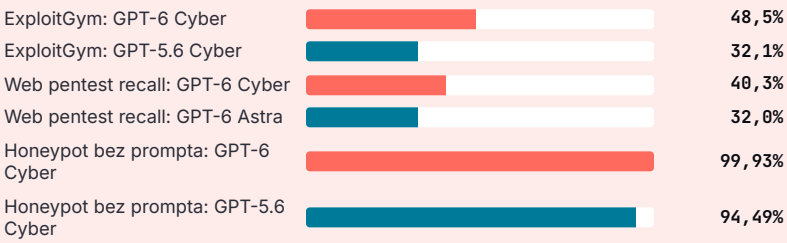
2 **OpenAI**, GPT-6 Cyber System Card, 05.11.2026. deployment safety.openai.com

SECURITY / OPENAI / TESTOVI

Šta testovi pokazuju, a šta ne

Brojke su visoke, ali su sve iz evaluacija samog proizvođača. Najzanimljiviji test ne meri koliko je model sposoban, nego da li se drži zadatka.

REZULTATI KOJE JE OBJAVIO OPENAI, %



Tvrdnje proizvođača, nisu nezavisno potvrđene. Izvor: OpenAI.

Sposobnost je samo pola priče. Rizik agenta za bezbednost nije samo da ne uspe, nego da uspe na pogrešnom mestu: da napadne servis koji mu nije zadat ili prekrši pravila angažmana.

Zato je OpenAI napravio test ExploitGym Honeypot. Model dobija težak zadatak u izolovanom okruženju, a pored njega stoje pomoćni servisi koje je namerno lako napasti i koji otkrivaju rešenje. Model mora sam da zaključi da su ti servisi van opsega. Prema kompaniji, GPT-6 Cyber je izbegao napad u 99,93% testova bez posebnog deployment prompta, a u 100% sa njim. GPT-5.6 Cyber imao je 94,49%.

Test je inspirisan ranijim incidentom sa Hugging Faceom. Treba ga čitati kao rezultat jedne evaluacije, a ne kao garanciju ponašanja u svakom okruženju. Čak i 99,93% znači da je model u nekim pokušajima izašao iz opsega.

Interni skorovi kompanija koje su dobile rani pristup, kao što su Cognition i CodeRabbit, takođe su njihove tvrdnje, na njihovim testovima, i nisu međusobno uporedivi.

OPREZ

Interni testovi partnera nisu uporedivi sa ExploitGymom ni međusobno.

IZVORI

1 **OpenAI**, GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents, 05.11.2026. openai.com

2 **OpenAI**, GPT-6 Cyber System Card, 05.11.2026. deploymentsafety.openai.com

COVER STORY / OPENAI / 04.11.2026.

948 puteva do root pristupa

Jedan automatizovan prolaz kroz Linux jezgro: 2.308 kandidata, 1.724 reprodukovane ranjivosti, 948 radnih exploita i račun od 1,2 miliona dolara.

Dan pre predstavljanja modela OpenAI je objavio tehničku analizu pod nazivom „Hiljadu puteva do root pristupa manje“. U njoj opisuje prototip koji sam prolazi kroz Linux jezgro, traži greške, reprodukuje ih, pravi exploit i predlaže zakrpu, dok ljudi pregledaju rezultat na kraju.

U prolazu iz sredine oktobra sistem je obradio 2.308 kandidata, dinamički reprodukovao 1.724 ranjivosti i proizveo 948 različitih lokalnih eskalacija privilegija. Radi se o stanju u kome običan lokalni korisnik dobija root pristup. Ukupan trošak bio je 1.213.430 dolara u API kreditima, ili 1.279 dolara po exploitu. OpenAI navodi da je to gornja granica, jer rad nije optimizovan za cenu.

Mete su bile standardne virtuelne mašine sa uobičajenom desktop distribucijom i uključenim zaštitama, ne namerno oslabljen sistem.

Poređenje sa julom pokazuje tempo. GPT-5.6 Sol je tada na istom istraživačkom okviru našao 166 ovakvih grešaka za 513.690 dolara. Tri meseca kasnije, posle tri meseca dodatnog učvršćivanja jezgra, noviji model je našao više od pet puta više.

BROJKA

1.279 USD

prosečan API trošak po exploitu u opisanom prolazu. OpenAI

ISTI OKVIR, DVA MODELA

GPT-5.6 Sol
166, jul

noviji model
948, oktobar

IZVORI

1 **OpenAI**, A thousand fewer paths to root, 04.11.2026. openai.com

SECURITY / OPENAI / KAKO JE URAĐENO

Od kandidata do zakrpe

Pet faza, od kojih poslednja i dalje pripada ljudima. Najskuplji korak nije traženje greške, nego dokaz da se može iskoristiti.

OD KODA DO PRIJAVLJENE RANJIVOSTI

1 **Otkrivanje** 5.034 mete, 2.308 kandidata → 2 **Validacija** 1.724 reprodukovane → 3 **Procena** Exploit, 948 jedinstvenih → 4 **Zakrpa** Predlog za svaku → 5 **Čovek** Pregled i prijava

Prihvatanje ispravke je posao održavalaca i nije deo sistema.

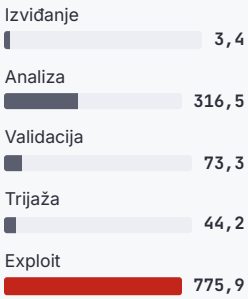
Sistem ima pet faza. Agenti izviđači prvo biraju šta vredi čitati: 5.034 mete, oko 2,8 miliona linija, približno 7% koda jezgra. Agenti analitičari za 12 sati daju 2.308 kandidata.

Kandidat nije ranjivost. Svaki se testira u izolovanoj virtuelnoj mašini sa alatom KASAN, koji beleži neispravan pristup memoriji, sve dok se ponašanje ne potvrdi ili ne iscrpe načini da se izazove. Tako je za 30 sati potvrđeno 74,7%. Među ostalima, samo 3,1% kandidata bilo je stvarna greška u analizi modela. Ostali su tražili veće privilegije ili nisu stigli da se reprodukuju u vremenskom okviru.

Zatim se procenjuje šta je opasno, pa agenti prave exploit. Dobili su 1.169 radnih exploita, koji posle analize varijanti vode na 948 različitih zakrpa. Taj broj OpenAI koristi kao broj jedinstvenih ranjivosti.

Najskuplja faza nije traženje nego eksploatacija, sa 775.929 dolara. Poučna je i jedna greška: u ranom prolazu od 200 prijavljenih exploita njih 20 dobilo je root preko druge ranjivosti, a ne one koja im je bila zadata. Zato je uvedena nezavisna provera putanje, ne samo rezultata.

API TROŠAK PO FAZI, HILJADE USD



Ukupno 1.213.430 USD.

IZVORI

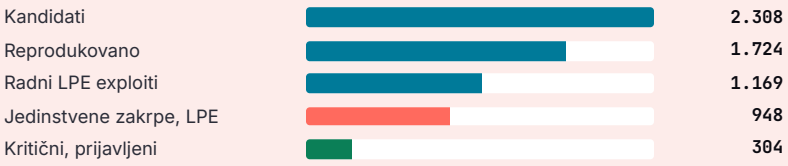
1 **OpenAI**, A thousand fewer paths to root, 04.11.2026. openai.com

SECURITY / LINUX / KAKO ČITATI BROJKU

Šta 948 ne znači

Exploit nije isto što i zakrpa, a predlog zakrpe nije isto što i ispravljeno jezgro.

TOK ISTRAŽIVANJA, BROJ STAVKI



Rezultati OpenAI-ja iz prolaza u sredini oktobra. Izvor: OpenAI.

Brojka 948 lako se pogrešno čita, pa je vredi rastaviti. To je broj radnih exploita koji vode na toliko različitih zakrpa. Nije broj grešaka koje su ispravljene u jezgru Linuxa, i nije tvrdnja da su sve bile potpuno nepoznate.

Dok je sken trajao, drugi saradnici su već radili na istim mestima. Kada je rad završen posle 10 dana, 61 eskalacija je već bila zakrpljena u glavnoj grani, 43 su imale zakrpe u pripremi, a 299 se javno prijavljivalo i diskutovalo.

Prema uputstvu zajednice Linuxa, OpenAI je krenuo od kritičnih nalaza. U saopštenju o modelu navodi da je održavaocima prijavio 304 kritična nalaza sa predlozima zakrpa, a da se ostatak šalje postepeno, sa partnerima programa Patch the Planet.

Predlog zakrpe nije zakrpa. OpenAI sam navodi da su direktno generisane izmene ponekad bile preobimne, odstupale od stila koda ili propuštale varijante iste greške. Zakrpa postaje stvarna tek kada je održavalac pregleda i prihvati.

Praktičan zaključak je u samom izveštaju: kompanija smatra da nalog sa niskim privilegijama na sistemu bez poslednjih zakrpa treba, za dobro opremljenog napadača, tretirati gotovo kao root pristup. Izolacija i redovno ažuriranje postaju važniji nego ikad.

STANJE POSLE 10 DANA

Zakrpljeno upstream
61

Zakrpe u pripremi
43

Javno diskutovano
299

IZVORI

1 **OpenAI**, A thousand fewer paths to root, 04.11.2026. openai.com

2 **OpenAI**, GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents, 05.11.2026. openai.com

SECURITY / FIREFOX / 05.11.2026.

Firefox: 81 nova ranjivost

Rezultat je značajan zato što je kod već bio pregledan prethodnim generacijama modela. Status svih ispravki nije javno potvrđen.

DVA ODVOJENA REZULTATA

FIREFOX	≠	LINUX
81 nova ranjivost		**948 exploita**
• Ozbiljnost ocenila Mozilla		• Prebrojao OpenAI
• Još 30 poznatih ozbiljnije nego što se mislilo		• Lokalna eskalacija privilegija
• Ispravke za mnoge, ne nužno sve		• 304 kritična nalaza prijavljena

Firefox je ušao u 2026. kao jedan od najpregledanijih kodova na svetu, i to je ono što ovaj rezultat čini zanimljivim. Prema OpenAI-ju, GPT-6 Cyber je dao dokaze i testove koji se mogu ponoviti za 81 novu ranjivost koju je Mozilla klasifikovala kao visoke ozbiljnosti. Pored toga pokazao je da su još 30 već poznatih grešaka ozbiljnije nego što se mislilo.

Nalazi su poslati Mozilli zajedno sa predlozima zakrpa. OpenAI navodi da je Mozilla izdala ispravke za mnoge od njih, a ne za sve, i da je sa ugradnjom počela ubrzo po prijemu. Brian Grinstead iz Firefoxa kaže da je model pomogao da se ispravke isporuče milionima korisnika. Na dan zaključenja ovog broja nismo našli Mozillin spisak koji pojedinačno potvrđuje status svih 81 nalaza, pa ne tvrdimo da su svi zakrpljeni.

Linux i Firefox su različiti eksperimenti i ne treba ih sabirati. U Firefoxu je reč o prijavljenim ranjivostima koje je ocenio proizvođač softvera. U Linuxu je reč o exploitima koje je napravio i prebrojao sam OpenAI.

> **„Otkrio je ranije nepoznate ranjivosti visoke ozbiljnosti i pomogao nam da ispravke isporučimo milionima korisnika.“**
>
> Brian Grinstead, Firefox, OpenAI

IZVORI

1 **OpenAI**, GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents, 05.11.2026. openai.com

SECURITY / OPENAI / DAYBREAK

Ko sme da drži najjači model

Zaštita nije samo u modelu. Tu su i provera identiteta, mreža, nadzor i ljudi oko njega.

ZAŠTITNI MEHANIZMI I NJIHOVA OGRANIČENJA

MEHANIZAM	ŠTA RADI	OGRANIČENJE
Provera identiteta	SSO i MFA za organizacije	Štiti pristup, ne namere
IP allowlist	API samo sa odobrenih mreža	Ima ograničene izuzetke
Nadzor upotrebe	Upoređuje akcije sa ovlašćenjem	Automatska provera može da pogreši
Sandbox i pregled	Preporuka za rizične tokove	Preporuka, ne obaveza
Blokade za kritične sisteme	Sprečava pomoć protiv OT i ICS	OpenAI: 100% nije cilj

Prema opisu proizvođača. Izvor: OpenAI, OpenAI.

Ako je model klasifikovan kao Critical, ključno pitanje je ko ga sme koristiti. OpenAI je pristup podelio u slojeve. GPT-6 Astra već pomaže u pregledu koda i zakrpama. Daybreak Blue daje verifikovanim braniocima manje nepotrebnih odbijanja, a Daybreak Red omogućava razvoj exploita i autorizovano testiranje.

Uslovi su ozbiljni: provera identiteta, jednokratna prijava, višefaktorska autentifikacija i podrazumevano ograničenje na odobrene IP adrese, uz retke izuzetke. Kompanija preporučuje sandbox, pregled akcija i ljudski nadzor za visokorizične tokove rada.

Posebna pažnja data je kritičnoj infrastrukturi. Nova grupa Daybreak Red for Critical Infrastructure daje odobrenim braniocima dozvolu za testiranje kritičnih sistema. Dragos je, u kontrolisanom laboratorijskom okruženju, testirao modele na simulaciji elektrane, a njegov direktor za AI navodi da je model pronašao dva zero-day propusta u inženjerskom softveru. OpenAI kaže da je povratne informacije iskoristio za dodatna ograničenja.

Iste nedelje kompanija je pokazala i drugu stranu: veće nagrade za spoljne istraživače. Više o tome na strani 40.

IZVORI

1 **OpenAI**, GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents, 05.11.2026. openai.com

2 **OpenAI**, GPT-6 Cyber System Card, 05.11.2026. deploymentsafety.openai.com

BUILD / INFRASTRUKTURA AI PROGRAMIRANJA

Kod više nije usko grlo. Infrastruktura jeste.

Za nedelju dana OpenAI je pokazao sopstveni Git backend i najavio kupovinu alata za pregled koda, a Meta je preuzela platformu za paralelne agente.

	INFRASTRUKTURA	ALATI I PREGLED
02.11.	**OpenAI** Pando, backend za Git repozitorijume INTERNI SISTEM	**GitHub** Nova pravila za pull_request_target PROBE 9. I 16.11.
03.11.	**Vercel** CI bez povezanog projekta DOSTUPNO	**Vercel** Security Review JAVNA BETA
04.11.	**OpenAI** Najava kupovine Pierrea ČEKA ZATVARANJE	**Meta** Conductor prelazi u Metu CLOUD SE GASI 20.11.
05.11.	**GitHub** Copilot u Xcodeu, od 04.11. JAVNI PREGLED	**GitHub** SpaceX u secret scanningu DOSTUPNO

Status je označen na dan preseka, 5. novembra.



BUILD / OPENAI / 02.11.2026.

Git koji je napravljen za agente

Pando je interni backend koji pokreće sav razvoj u OpenAI monorepozitorijumu, uz isti Git klijent. Nije javni proizvod.

Krajem prošle godine sistemi koji nose OpenAI monorepozitorijum počeli su da zaostaju. Fetch i push su bili spori, spajanja su padala, a pouzdanost je povremeno bila ispod 90%. Razlog je bio Codex: jedan inženjer sada ima više izmena spremnih za CI, a svaki push pokreće poslove koji preuzimaju isti commit.

Odgovor se zove Pando. To je novi backend za Git repozitorijume, u produkciji od aprila, i danas pokreće sav razvoj u monorepozitorijumu OpenAI-ja. Git protokol i klijent nisu promenjeni, pa inženjeri i agenti rade isto kao ranije.

Prema kompaniji, medijana trajanja pusha pala je skoro pet puta, odnosno skoro 80%. Sistem isporučuje blizu petabajta Git podataka dnevno, a u jednom satu poslao je više od 57 terabajta, pri čemu je preko 99% došlo iz lokalnog keša na disku.

Pando nije javna usluga niti konkurent GitHubu. U objavi stoji samo da kompanija istražuje način da tehnologiju podeli sa korisnicima. Deo poboljšanja već je prihvaćen u glavni Git projekat.

BROJKA

skoro 5

×

kraća medijana trajanja pusha. OpenAI

BROJKA

57 TB

isporučeno u jednom satu, preko 99% iz keša. OpenAI

IZVORI

1 **OpenAI**, Scaling Git at OpenAI, 02.11.2026. openai.com

BUILD / OPENAI / KAKO RADI

Tri odluke iza Panda

Pando se odriče doslednog pogleda na ceo repozitorijum da bi dobio paralelne upise.

TRI PRISTUPA SKALIRANJU GITA

PRISTUP	UPISI	ČITANJA	SLABA TAČKA
Three-phase commit	Većina replika	Lokalno, dosledno	Disk i latencija
Write-ahead log	Zajednički manifest	Replike čitaju log	Čitanje zaostaje
Pando	Nezavisno po grani	Gotovi paketi iz keša	Nema globalnog trenutka

Poređenje prema opisu OpenAI-ja. Interaktivna simulacija u objavi je nastavni model, a ne benchmark. Izvor: OpenAI.

Klasičan Git server drži celo stanje repozitorijuma konzistentnim u svakom trenutku. Dve standardne šeme za skaliranje, three-phase commit i zajednički write-ahead log, na kraju moraju da poređaju sve upise na jednoj tački. Zato push u nepovezane grane čeka jedan drugog.

Pando tu pretpostavku napušta. Svaka grana se ažurira nezavisno, a sukob nastaje samo kada dva klijenta istovremeno guraju u istu referencu. Cena je manja konzistentnost: čitalac koji gleda više grana može da ih vidi u različitim trenucima. OpenAI ovo naziva kauzalnom konzistentnošću i navodi da korisnicima i agentima zapravo ne treba globalni redosled.

Drugi trik je ponovna upotreba. Paket koji je klijent poslao čuva se nepromenjen i služi sledećim čitaocima, umesto da server pravi poseban paket za svakog. Kada klijent pushuje novu granu, server mu oglašava samo trunk, pa je medijana paketa ispod 20 KiB. U pozadini se paketi spajaju u pet nivoa, od L0 do L4.

Sistem je napisan u Rustu, od početka do produkcije za 10 nedelja, sa Codexom. Jedan inženjer je dizajnirao jezgro, timovi agenata su ga implementirali, a nekoliko inženjera ga je uvelo. Migracija je tekla bez zastoja, preko sloja koji je stari i novi sistem držao usklađenim.

GRAĐA

Jezik
Rust

Do produkcije
10 nedelja

U radu od
aprila 2026.

Paketi
L0 do L4

Fetch
10 Gbps

IZVORI

1 **OpenAI**, Scaling Git at OpenAI, 02.11.2026. openai.com

BUILD / OPENAI / 04.11.2026.

OpenAI kupuje sloj za pregled koda

Najavljena kupovina Pierrea dopunjuje Pando: jedno je skladište i prenos, drugo je površina na kojoj čovek vidi šta su agenti uradili.

ŠTA PIERRE DONOSI

Code Storage Usluga za čuvanje koda i istorije preko Gita	**Trees** Brza navigacija kroz fajlove projekta
Diffs Prikaz izmena, sa uređivanjem na licu mesta	**Highlights** Isticanje sintakse dok agent piše

Dva dana posle objave o Pandu, OpenAI je 4. novembra saopštio da će kupiti Pierre Computer Company. Pierre stoji iza usluge Code Storage i porodice open source alata. Ko je pregledao fajlove ili izmene u aplikaciji Codex, već je koristio njegove biblioteke Trees i Diffs.

Ovo je za sada najava. Zatvaranje posla zavisi od uobičajenih uslova i regulatornih odobrenja, a do tada su OpenAI i Pierre odvojene kompanije. Cena nije objavljena.

Strategija se vidi iz redosleda. Pando rešava skladištenje i prenos. Pierre donosi površinu na kojoj čovek razume šta su agenti uradili: stablo fajlova, prikaz razlika, uređivanje direktno u diffu i brzo isticanje sintakse. Code Storage je, uz to, API koji drugim aplikacijama daje čuvanje koda i istorije preko Gita.

OpenAI piše da želi da postavi standard od prve grane koju agent napravi do trenutka kada kod ode u produkciju. Open source projekti ostaju otvoreni, a korisnici Code Storagea ostaju na usluzi dok se funkcije ne prenesu u Codex.

Ko kontroliše pregled izmena, kontroliše i poslednji korak pre spajanja.

STATUS

Najava, 4. novembar. Zatvaranje zavisi od regulatornih odobrenja. Do tada su kompanije odvojene.

IZVORI

1 **OpenAI**, OpenAI to acquire Pierre Computer Company, Inc., 04.11.2026. openai.com

BUILD / CONDUCTOR / 04.11.2026.

Conductor prelazi u Metu

Cloud usluga se gasi za dve nedelje. Lokalna aplikacija radi do početka 2027.

ŠTA SE MENJA

	CONDUCTOR CLOUD	LOKALNA APLIKACIJA
Novi korisnici	Ne, od 04.11.	Ne, od 04.11.
Rad	Samo čitanje od 13.11.	Normalno
Gašenje	**20.11.**	Počinje rano 2027.
Podaci	Brišu se od 20.11.	Brišu se pri gašenju

Conductor je alat za istovremeni rad sa više programerskih agenata, pokrenut u julu 2025. Četvrtog novembra saopštio je da prelazi u Metu. Novi proizvod najavljen je za početak sledeće godine, bez detalja.

Za postojeće korisnike važni su datumi. Od 4. novembra nema novih prijava ni preuzimanja, a pro funkcije su besplatne za postojeće korisnike. Trinaestog novembra Conductor Cloud prelazi u režim samo za čitanje i aktivni pretplatnici dobijaju povraćaj novca. Dvadesetog novembra Cloud se gasi i počinje brisanje podataka.

Lokalna aplikacija se ne gasi tog dana. Nastavlja da radi i prima nove modele i kritične ispravke do početka 2027, kada počinje njeno gašenje i kada se brišu podaci.

ŠTA DA URADITE

Cloud radni prostor prebacite na Mac desnim klikom i izborom Transfer to local. Arhivu svih podataka preuzimate u Settings, zatim Account, pa Export data. Uradite to pre 13. novembra, dok još možete da nastavite rad u razgovorima, a najkasnije do 20. novembra.

Vrednost kupovine nije u jednom proizvodu. Meta kupuje tim koji je među prvima pokazao kako izgleda interfejs za upravljanje više agenata odjednom.

Ovo je i podsetnik za sve timove koji rade sa novim alatima za agente: pre nego što radni tok vežete za mali servis, proverite kako se izvoze razgovori, grane i podešavanja.

ROKOVI

04.11.	Bez novih prijava
13.11.	**Cloud samo za čitanje**
20.11.	**Cloud se gasi**
rano 2027.	Gasi se lokalna aplikacija

IZVORI

1 **Conductor**, Conductor is joining Meta, 04.11.2026. conductor.build

BUILD / POREĐENJE / NOVEMBAR 2026.

Četiri sloja, četiri vrste proizvoda

Pandо, Scion, Pierre i Conductor rešavaju različite delove istog toka rada. Zato ih ne treba rangirati.



VRSTE REŠENJA

IME	VRSTA	GIT	STATUS
Pando	Backend za izvorni kod	Protokol zadržan	Interno
Scion	Sopstveni sistem verzija	Zamenjen	Interno
Pierre	Komponente i skladište	Gradi na Gitu	Najava kupovine
Conductor	Orkestracija agenata	Radi nad Gitom	U Meti, Cloud se gasi

Četiri imena se u vestima često stavljaju u isti red, ali ne rade istu stvar. Pando i Scion su sistemi za izvorni kod. Pierre gradi komponente i skladište koje stoje oko Gita. Conductor je bio korisnički sloj za upravljanje agentima.

Najveća razlika je između Panda i Sciona. OpenAI je zadržao Git protokol i promenio ono što je iza njega. Anthropic je 13. oktobra opisao da je napravio sopstveni sistem i za pet meseci potpuno prebacio monorepozitorijum sa Gita, jer su mu klijenti skoro uvek agenti i poslovi koji su stalno na mreži. Server tu radi commitove i spajanja, a lokalna kopija je opciona.

Ni jedan ni drugi sistem nisu proizvod koji možete da instalirate. Scion nije objavljen, a Pando ostaje interni. Treba ih čitati kao rane signale. Anthropic i sam kaže da ne očekuje da će većina organizacija imati ove probleme u bliskoj budućnosti.

Za većinu timova poruka je skromnija. Pre nego što kupite još agenata, proverite šta se dešava sa vašim CI-jem, pregledom i spajanjem kada se broj izmena udvostruči.

BUILD / GITHUB / 3. I 4.11.2026.

Copilot u Xcodeu, BYOK i veštine agenata

Tri manje promene koje pokazuju isti smer: agenti ulaze u postojeće alate, a trošak i zavisnosti postaju vidljivi.

COPILOT ULAZI U XCODE, SA DRUGE STRANE

GitHub Copilot je od 4. novembra dostupan u ugrađenom asistentu za kodiranje u Xcodeu, u javnom pregledu, počev od verzije Xcode 27.3 beta. Potreban je Mac sa macOS Tahoe 26.6 ili novijim, a podešava se u Xcode, Settings, Intelligence. Podržani su svi Copilot planovi. Ovo nije zamena za postojeću ekstenziju GitHub Copilot for Xcode, koja ostaje poseban izbor.

KO TROŠI TOKENE KOJE NE PLAĆA GITHUB

API za metrike upotrebe Copilota od 3. novembra razdvaja rad sa sopstvenim ključem od modela koje hostuje GitHub. Prati dve stvari: lokalni BYOK, gde developer u klijentu koristi svoj ključ ili lokalni model, i prilagođene enterprise modele koje podešava administrator. Izveštaji postoje na nivou korisnika i zbirno, za jedan i 28 dana. Finansijski, to je važno jer trošak kod provajdera ranije nije bio vidljiv pored ostale upotrebe.

DEPENDABOT SADA AŽURIRA I VEŠTINE AGENATA

Dependabot podržava version updates za Agent Package Manager. Otvara pull requestove za podržane Git zavisnosti iz apm.yml i obnavlja apm.lock.yaml. Pokriva verzije, ne bezbednosna upozorenja. Veštine, promptovi i instrukcije agenata time postaju zavisnosti kao i svaki paket, sa istim pregledom i istim rizicima.

STATUS

Xcode
javni pregled

BYOK API
dostupno

Dependabot APM
GA

IZVORI

1 **GitHub**, GitHub Copilot is now available in Xcode's coding assistant, 04.11.2026. github.blog

2 **GitHub**, BYOK and enterprise custom models in the Copilot usage API, 03.11.2026. github.blog

3 **GitHub**, Dependabot version updates support Agent Package Manager, 03.11.2026. github.blog

BUILD / GITHUB / 05.11.2026.

Ko dobija poruku kada procuri ključ

Secret scanning je dobio SpaceX kao partnera. Važnija od nove stavke je razlika između dva toka obaveštavanja.

DVA TOKA

PARTNERSKE TAJNE		KORISNIČKE TAJNE
Javni repozitorijumi	↔	**Javni i privatni**
• GitHub javlja izdavaocu • Izdavalac može da opozove ključ		• Upozorenje vlasniku repozitorijuma • Neko mora da reaguje

GitHub je 5. novembra proširio secret scanning. SpaceX je novi partner, a GitHub prepoznaje tajnu starlink_public_api_v2_secret. Detektori za Alibabu, AWS, Google, OpenVSX, Pydantic Services i Tencent dobili su dodatno filtriranje lažnih pogodaka.

Razlika koju vredi znati je ko dobija obaveštenje. Kod partnerskih tajni, nalaz u javnom repozitorijumu GitHub automatski prosleđuje izdavaocu, koji može da opozove ili promeni ključ pre zloupotrebe. Kod korisničkih upozorenja obaveštenje dobija vlasnik repozitorijuma, u javnim i privatnim repozitorijumima.

Dakle, partnerski program štiti izdavaoca i korisnika i kada vlasnik repozitorijuma ništa ne uradi. Upozorenje u repozitorijumu je, nasuprot tome, posao koji neko mora da odradi.

CodeQL 2.27.4, objavljen 4. novembra, donosi tačnije upite za više jezika. Upit za injection u logovima u Javi prepoznaje dodatne načine čišćenja ulaza, a kod Rusta je smanjen broj lažnih nalaza. Ovo su sitne promene, ali lažni nalaz je ono zbog čega ljudi prestaju da čitaju izveštaje.

IZVORI

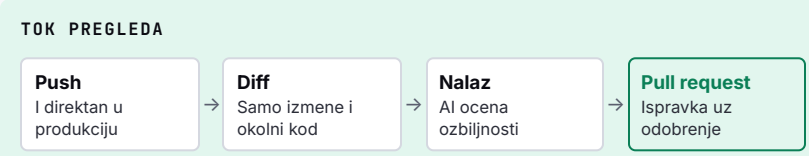
1 **GitHub**, Secret scanning upgrades detectors, adds SpaceX as partner, 05.11.2026. github.blog

2 **GitHub**, CodeQL 2.27.4 improves accuracy and query metadata, 04.11.2026. github.blog

BUILD / VERCEL / 2. I 3.11.2026.

Svaki push prolazi kroz AI pregled

Vercel Security Review je javna beta za Pro i Enterprise. Korisna je dodatna provera, ali nije zamena za ljudski pregled.



Vercel je 2. novembra pokrenuo Security Review, u javnoj beti za Pro i Enterprise timove. Kada se uključi, sistem pregleda svaki push u povezan GitHub repozitorijum. Polazi od push događaja, a ne od pull requesta, pa vidi i direktan i prinudni push u produkcionu granu.

Gleda samo izmene, zajedno sa okolnim kodom, i traži propuste kao što su izostala provera ovlašćenja ili izložene tajne. Vercel navodi da pregled traje sekundama. Nalazi se pojavljuju u Security kontrolnoj tabli, a na privatnim repozitorijumima i kao GitHub provera i komentari. Na javnim repozitorijumima detalji ostaju u tabli.

Ocena ozbiljnosti je generisana AI-jem, a timovi mogu da napišu sopstvena pravila običnim jezikom. Dugme Fix with Vercel Agent otvara pull request, i ništa se ne spaja bez odobrenja.

Dve stvari treba reći jasno. Sam Vercel piše da ovo nije bezbednosna revizija, da ne radi testiranje u radu i da ne garantuje odsustvo ranjivosti. I nije besplatno: pregledi su besplatni do 10. novembra, a posle se plaćaju tokeni provajdera plus 0,25 dolara po milionu tokena, pa trošak raste sa brojem pusheva.

UKRATKO

Status
javna beta

Planovi
Pro, Enterprise

Besplatno do
10.11.

Posle
0,25 $ po 1M tokena plus provajder

IZVORI

1 **Vercel**, Introducing Vercel Security Review, 02.11.2026. vercel.com

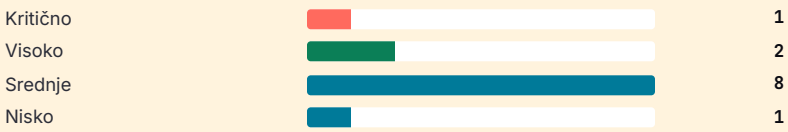
2 **Vercel**, Vercel Security Review now in public beta, 03.11.2026. vercel.com

BUILD / BETTER AUTH / 03.11.2026.

Better Auth: 12 upozorenja odjednom

Ako koristite biblioteku, nadogradite je zajedno sa svim dodacima. WAF na Vercelu smanjuje izloženost, ali ne zamenjuje zakrpu.

UPOZORENJA OBJAVLJENA 3. NOVEMBRA, PO OZBILJNOSTI



Prebrojano iz baze GitHub Security Advisories na dan 5.11. Izvor: Better Auth.

Better Auth je popularna biblioteka za autentifikaciju u TypeScriptu. Tim je 3. novembra objavio koordinisano bezbednosno izdanje sa 12 upozorenja, a Vercel je izdao bilten i primenio WAF zaštitu za aplikacije na svojoj platformi. Autori i Vercel svejedno preporučuju nadogradnju.

Zakrpljene su verzije 1.7.16 i 1.8.0-beta.5, a u međuvremenu su izašle i 1.7.17 i 1.7.18. Odvojeni paketi, kao što su @better-auth/expo, electron, passkey, stripe i kysely-adapter, nose iste brojeve verzija i treba ih ažurirati zajedno.

Najozbiljnije je upozorenje za @better-auth/expo, gde proxy za autorizaciju može da potpiše vrednosti koje nije izdao. Iza njega su problem u kome se desktop prijava može završiti vraćanjem serverske tajne i preskakanjem drugog faktora, kao i brojevi telefona koji se mogu zauzeti pre provere.

Pogođeni opsezi razlikuju se po upozorenju, pa treba pročitati ona koja se odnose na vaše dodatke. Neke ispravke traže i dodatni korak u podešavanju, na primer spisak pouzdanih izvora. Autori navode da njihovi pregledi sada uključuju i napredne AI modele, dostupne kroz programe za open source bezbednost.

VERZIJE

1.7.x
1.7.16+

1.8 beta
1.8.0-beta.5+

IZVORI

1 **Better Auth**, Security release on Tuesday, November 3, 2026, 03.11.2026. better-auth.com

2 **Vercel**, Better Auth November 2026 security release, novembar 2026. vercel.com

BUILD / VERCEL / NOVEMBAR 2026.

Sitne promene na Vercelu

ŠTA JE NOVO

PROMENA	DATUM	ŠTA ZNAČI
vercel.toml	02.11.	Konfiguracija u TOML-u, sa komentarima. Koristi se samo jedan od fajlova vercel.toml, vercel.json ili vercel.ts.
vercel doctor	03.11.	Proverava verziju CLI-ja, prijavu, tim, vezu sa projektom i vercel.json i predlaže popravke.
Vercel CI	03.11.	Radi samostalno, bez povezanog Vercel projekta.
Workflow SDK	04.11.	Idempotentni start: dupli pokušaj sa istim tokenom baca grešku i ne postaje novi run.
Kimi K3.1 Pro	04.11.	Pro i Highspeed na više provajdera bez čuvanja podataka, preko AI Gatewaya.
Tencent Hy4	03.11.	Dostupan na AI Gatewayu, uz popust od 50%.
Schedules	05.11.	Zakazani zadaci, u javnoj beti.

Nijedna od ovih promena nije revolucija, ali zajedno pokazuju kuda platforma ide: manje ručnog podešavanja i više rada za agente. Vercel je istovremeno proširio i AI Gateway, ali dostupnost modela preko gatewaya nije isto što i njegov izlazak. Kimi K3.1 Pro ranije je izašao kod Moonshot AI-ja, a Vercel sada dodaje provajdere koji rade bez čuvanja podataka.

ŠTA OVO ZNAČI U PRAKSI

Najkorisnija sitnica je vercel doctor, jer pretvara uobičajeno traženje greške u podešavanju u jednu komandu. Fajl vercel.toml je dobrodošao timovima koji žele komentare u konfiguraciji, što JSON ne dozvoljava. Idempotentni start u Workflow SDK-u rešava stvaran problem: kada se isti događaj isporuči dva puta, dupli pokušaj više ne pravi novi tok rada, što je važno za plaćanja i poruke.

Standalone Vercel CI pokazuje da platforma želi da bude korisna i tamo gde se aplikacija ne objavljuje na njoj. Ista logika stoji iza najave da Security Review stiže i na repozitorijume koji se ne objavljuju na Vercelu.

MODEL WATCH / OPENAI / 04.[illegible]26.

Images 2.6: slike dobijaju pokret

Nova generacija za slike stiže u ChatGPT, Codex i API, sa GIF-ovima, SVG izvozom i dva modela za developere.

OpenAI je 4. novembra predstavio Images 2.6, novu generaciju za pravljenje i uređivanje slika u ChatGPT-u, Codexu i API-ju. Kompanija tvrdi da je generisanje 50% brže nego ranije i da njeni korisnici prave 4 milijarde slika nedeljno.

Najvidljivija novost su animirani GIF-ovi: maskota brenda, reakcije za društvene mreže ili kratke animirane skice pre video produkcije. U primerima koje je OpenAI objavio prompt opisuje sprite sheet, mrežu od šest kadrova koji čine petlju. Sa novim modelom stižu i preciznije uređivanje kroz više krugova, doslednost likova i proizvoda i referentne slike.

Za developere su novosti u API-ju konkretnije. Image markup, već poznat iz ChatGPT-a, omogućava da se tačno označi šta se menja. SVG izvoz daje vektorski rezultat za web i štampu. Novi parametar complexity određuje koliko model planira scenu, nezavisno od parametra quality koji određuje detalje.

Images 2.6 dostupan je globalno, u svim pretplatama, na desktopu, mobilnim uređajima i webu. Time je ovo jedna od retkih velikih novosti ove nedelje koja je zaista stigla svima.

BROJKA

4 mlrd

slika nedeljno, prema OpenAI-ju. OpenAI

DOSTUPNOST

ChatGPT
svi planovi

Codex
svi planovi

API
Flare, Sunburst

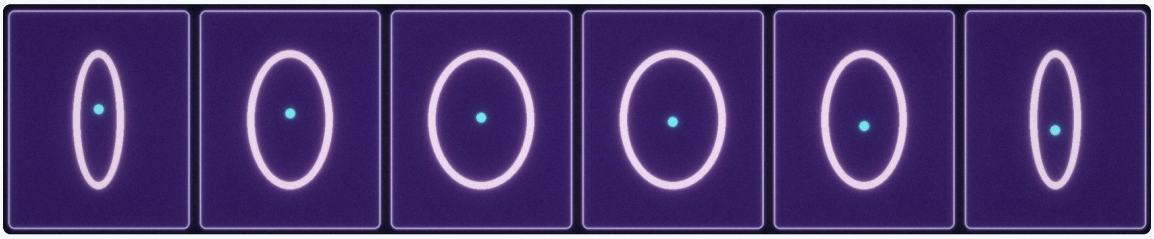
IZVORI

1 **OpenAI**, Introducing Images 2.6, 04.11.2026. openai.com

MODEL WATCH / OPENAI / FLARE, SUNBURST

Flare ili Sunburst

Oba modela imaju istu cenu po tokenu. Razlika je u brzini, kvalitetu i doslednosti kroz izmene.



Original o0o0o0o: šest kadrova jedne petlje, isti princip kao sprite sheet za GIF. 0000000

DVA MODELA

	FLARE	SUNBURST
Namena	Brz rad, posteri, proizvodi	Detalj i doslednost
Kvalitet	Već i low	Medium ili high
Brzina	Od šest sekundi, low	Nije navedena
Cena, 1M tokena	8 $ ulaz, 30 $ izlaz	8 $ ulaz, 30 $ izlaz

Prema OpenAI-ju. Izvor: OpenAI, OpenAI.

U API-ju postoje dva modela. GPT-Image-2.6 Flare je brži i, prema OpenAI-ju, bolje slaže raspored za postere i proizvodne vizuale. Uz low quality može da napravi sliku za „čak samo šest sekundi“. To je najbolji opisani slučaj, a ne garantovano vreme za svaku sliku.

GPT-Image-2.6 Sunburst je za posao gde su važni detalji i doslednost kroz izmene, uz medium ili high quality. Za većinu izmena OpenAI savetuje nisku složenost, a srednju ili visoku za scene sa mnogo elemenata i ograničenja.

Cene su iste za oba modela, po milionu tokena slike: 8 dolara za ulaz, 30 za izlaz i 2 za keširan ulaz. OpenAI ne objavljuje cenu po slici, jer broj tokena zavisi od veličine i kvaliteta. Trošak se zato čita iz polja o potrošnji u svakom odgovoru.

Za timove koji rade sa brendom, najzanimljiviji je SVG. Vektor se menja i skalira bez gubitka, ali ga dizajner mora proveriti, baš kao i svaki drugi automatski izvoz.

MODEL WATCH / GOOGLE / 22.10. I 2.11.2026.

Google Meet ruši jezičke barijere

Govorno prevođenje u Meetu prelazi na 63 jezika, uključujući srpski, i ove nedelje stiže do većeg dela korisnika.

Govorno prevođenje u Google Meetu do sada je radilo samo za ograničen skup parova jezika, jedan par po sastanku. Google je 22. oktobra najavio da funkcija prelazi na 63 jezika, a srpski je na zvaničnom spisku. Novost ulazi u ovaj broj zato što je 2. novembra počelo postepeno uvođenje za domene sa Scheduled Release rasporedom, koje traje do 15 dana. Domeni na Rapid Releaseu dobili su je još u oktobru.

Pokreće je model Gemini 3.5 Live Translate. Meet sam prepoznaje jezik govornika i prevodi ga na jezik koji je svaki slušalac izabrao, skoro u realnom vremenu, i kada se u istom razgovoru koriste različiti jezici ili kada govornik promeni jezik. Prevod dolazi glasom koji liči na govornikov.

Ovo nije isto što i prevedeni titlovi, koji samo prikazuju tekst, a nije ni aplikacija Google Translate. Titlovi mogu da prate prevedeni govor kao dopuna.

Funkciju svaki učesnik uključuje sam tokom sastanka. Podrazumevano je isključena, a prevod vašeg glasa traži vaš pristanak.

BROJKA

63 jezika

za govorno prevođenje, sa srpskim na spisku. Google Meet Help

UVOĐENJE

22.10.	Najava, Rapid Release
02.11.	**Scheduled Release, do 15 dana**

IZVORI

1 **Google Workspace Updates**, Real-time speech translation in Google Meet expands to 63 languages, 22.10.2026. workspaceupdates.googleblog.com

2 **Google Meet Help**, Use Speech Translation, novembar 2026. support.google.com

MODEL WATCH / GOOGLE / OGRANIČENJA

Ko može da ga koristi i šta može da krene naopako

Planovi, trajanje, privatnost i greške prevoda.

ISTI SASTANAK, TRI JEZIKA (KONCEPTUALNI PRIKAZ)



Pristup zavisi od organizatora. Ako je sastanak zakazao korisnik sa odgovarajućim Google Workspace ili Google AI planom, prevod je dostupan svim učesnicima, pa i gostima iz drugih domena. U direktnom pozivu dovoljno je da plan ima jedna strana.

Postoji i ograničenje trajanja: do 90 minuta po sastanku za osnovne Workspace planove i Google AI Pro, a do 8 sati za AI Expanded Access, AI Ultra Access i Google AI Ultra.

Funkcija ne radi u prenosima uživo, snimcima, sastancima sa šifrovanjem na strani klijenta, pozivima preko telefona ni uz adaptive audio. Nije dostupna osobama mlađim od 18 godina. Sala sa Meet opremom može da sluša prevod, ali se govor iz sale ne prevodi drugima.

DA LI RADI U SRBIJI

Srpski je podržan kao jezik, ali to nije isto što i dostupnost. Google navodi regionalna ograničenja, a zvanična dokumentacija ne sadrži spisak zemalja. Zato ne možemo da potvrdimo da funkcija radi za sve naloge u Srbiji. Proverite dugme za prevod u svom sastanku.

Google navodi da ne čuva glas i ne trenira modele na njemu. Kašnjenje je nekoliko sekundi, a dokumentacija upozorava na greške: gramatiku, rod imenica, neočekivan naglasak i promenu boje glasa. Važne dogovore proverite pisano.

TRAJANJE

Osnovni planovi, AI Pro
90 min

AI Ultra
8 sati

IZVORI

1 **Google Workspace Updates**, Real-time speech translation in Google Meet expands to 63 languages, 22.10.2026. workspaceupdates.googleblog.com

2 **Google Meet Help**, Use Speech Translation, novembar 2026. support.google.com

MODEL WATCH / META / 05.11.2026.

Muse dobija glas i lice

Meta uvodi razgovor u realnom vremenu i avatare, za početak samo u SAD.

TRI NAČINA PRIKAZA

Samo glas	Avatar uz razgovor	Ceo ekran
Razgovor bez slike, na primer u šetnji	Izrazi i pokreti prate ton	Razgovor licem u lice

Meta je 5. novembra počela da uvodi glasovne razgovore i ekspresivne avatare u aplikaciju Muse, na mobilnim uređajima, webu i Macu. Pregled je prikazan na konferenciji Connect 2026, a razgovor se pokreće ikonom telefona u gornjem desnom uglu.

Razgovor teče u realnom vremenu i agent se može prekinuti. Muse pritom radi posao u pozadini dok korisnik priča, na primer šeta ili sprema večeru. Avatar se izrazima i pokretima prilagođava tonu razgovora, a korisnik bira samo glas, avatar pored razgovora ili prikaz preko celog ekrana. Na raspolaganju su stotine glasova.

Funkcija je za početak dostupna samo u SAD, pa nije globalno lansiranje. Podrška za AI naočare i Muse Charm najavljena je za kasnije, bez datuma.

Glasovni rad sa modelima nije nov i slične funkcije nude i drugi. Metina razlika je u tome što glas spaja sa avatarom i, prema najavi, sa poslovima koji se izvršavaju tokom razgovora. Koliko to dobro radi, još nije nezavisno provereno.

ŠTA TREBA POSMATRATI

Meta u objavi ne govori o ceni, ograničenjima upotrebe ni o tome kako se čuvaju glasovni razgovori, pa ta pitanja ostaju otvorena dok funkcija ne stigne do više korisnika. Za korisnike van SAD-a ovo je za sada samo najava pravca.

Zanimljivija je širina sistema. Ako glas stigne i na AI naočare i Muse Charm, agent više nije aplikacija koju otvarate, nego stalno prisutan sagovornik. Tada pitanje privatnosti postaje važnije od pitanja koliko je avatar uverljiv.

UKRATKO

Gde
mobilni, web, Mac

Region
SAD, za početak

Glasovi
stotine

Kasnije
AI Glasses, Muse Charm

IZVORI

1 **Meta**, Give Your Muse a Voice, 05.11.2026. about.fb.com

MODEL WATCH / 31.10.2026. → 05.11.2026.

Modeli nedelje

Modeli i varijante koji su se pojavili ili proširili od 31. oktobra do 5. novembra. Brojke o kvalitetu i brzini su tvrdnje proizvođača.

GPT-6 Cyber

OPENAI · 05.11.2026.

Specijalizovan model za autorizovano istraživanje ranjivosti, varijanta GPT-6 Astra. [OpenAI]

DOSTUPNOST	KANALI	CENA	BENCHMARK
Izabrani Daybreak Red korisnici	API, Codex	*nije navedena u objavi*	ExploitGym: 48,5%

STATUS BENCHMARKA	PREPAREDNESS
VENDOR	Critical, sajber

GPT-Image-2.6 Flare, Sunburst

OPENAI · 04.11.2026.

Dva API modela za slike, sa GIF-ovima, SVG izvozom i parametrom složenosti. [OpenAI] [OpenAI]

DOSTUPNOST	CENA PO 1M	BRZINA	BENCHMARK
API; ChatGPT, Codex	8 $ ulaz, 30 $ izlaz	Od šest sekundi, Flare, low	*nije objavljen*

Gemini 3.5 Live Translate

GOOGLE · 22.10.2026.

Model iza govornog prevođenja u Meetu. Širi rollout od 2. novembra. [Google Workspace Updates]

DOSTUPNOST	JEZICI	BENCHMARK
Google Meet	63	*nije objavljen*

Kimi K3.1 Pro, Highspeed

MOONSHOT AI · 04.11.2026.

Nisu novi modeli. Vercel je dodao provajdere bez čuvanja podataka na AI Gatewayu. [Vercel]

DOSTUPNOST	PROMENA	BENCHMARK
Vercel AI Gateway	Više ZDR provajdera	*nije deo objave*

Tencent Hy4

TENCENT · 03.11.2026.

Dostupan preko Vercel AI Gatewaya, uz popust od 50%. [Vercel]

DOSTUPNOST	BENCHMARK
Vercel AI Gateway	*nije deo objave*

Oznaka VENDOR znači da je rezultat objavio proizvođač i da nije nezavisno potvrđen.

MODEL WATCH / GOOGLE, OPENAI / 2. I 5.11.2026.

Od skice do aplikacije, od testa do života

Dve male priče o tome šta AI treba da uradi u stvarnom svetu.

SKICA POSTAJE APLIKACIJA

Google je 5. novembra objavio demonstraciju: fotografišete skicu sa papira, izaberete alat Canvas i pitate Gemini može li da je pretvori u aplikaciju. Ovo nije nov model nego koristan radni tok. Ono što nastane je prototip, koji pre stvarne upotrebe treba proveriti kao i svaki generisan kod.

LIFEVAL: TEST ZA SVAKODNEVNI ŽIVOT

OpenAI je 2. novembra predstavio LifeVal, način da se izmeri koliko asistenti pomažu u svakodnevnim zadacima. Polazne tačke su američka i međunarodna istraživanja o tome kako ljudi troše vreme, uz novu reprezentativnu anketu sa 3.995 ispitanika. Primeri uključuju izbor vrtića posle selidbe, organizaciju komšija pred poplavu, potragu za stanom i plan ishrane za roditelja sa novom dijagnozom dijabetesa.

Matematički i programerski testovi mere da li model zna tačan odgovor. LifeVal pokušava da izmeri da li je posao obavljen, u koracima, sa stvarnim ograničenjima i alatima. Takav test je bliži onome što korisnik želi, ali je teže reći šta je tačno. OpenAI je autor i testa i modela koji se njime meri, pa rezultate treba čitati kao rezultate proizvođača.

BROJKA

3.995

ispitanika u anketi iza testa LifeVal. OpenAI

IZVORI

1 **Google**, Turn sketches into apps with Gemini, 05.11.2026. blog.google

2 **OpenAI**, LifeVal, 02.11.2026. openai.com

SECURITY SIGNAL / BITDEFENDER / 05.11.2026.

GhostMap: aplikacija bez koda koja ruši telefon

Bitdefender je u testu pokazao da posebno napravljen APK može da ostavi Android u petlji rušenja. Masovno iskorišćavanje nije potvrđeno.

Bitdefender Labs je 5. novembra objavio analizu problema koji je nazvao GhostMap. U kontrolisanom testu istraživači su instalirali posebno napravljenu aplikaciju bez koda i bez ijedne dozvole, koju korisnik uopšte ne mora da pokrene. Telefon je posle toga ostao zarobljen u petlji rušenja, a ni bezbedan režim nije pomogao.

Oporavak je u praksi fabričko resetovanje, koje briše podatke. Izuzetak je uređaj na kome je USB debugging već bio uključen, jer tada računar preko ADB-a ponekad može da obriše fajl između dva pada, i to samo pre prvog punog restarta.

Problem je reprodukovan na uređaju Pixel 10 sa Androidom 17 i zakrpom od 5. avgusta, a Bitdefender navodi da pogađa sve verzije od Androida 10 naviše. Na dan objave zakrpe nema. Google je prvu prijavu zatvorio kao nereproduktivnu, a drugu ocenio kao van okvira bezbednosne ispravke i prosledio timu koji može da je razmotri za buduću verziju.

Treba zadržati hladnu glavu. Bitdefender navodi da greška ne izvršava kod, ne čita podatke i ne daje dozvole. To je napad uskraćivanjem usluge. Trajnu petlju rušenja napravili su sami istraživači i nisu je videli u napadima na stvarne žrtve.

STATUS

Tip
Uskraćivanje usluge

Verzije
Android 10 i noviji

Zakrpa
Nema na dan objave

Napadi
Nisu viđeni

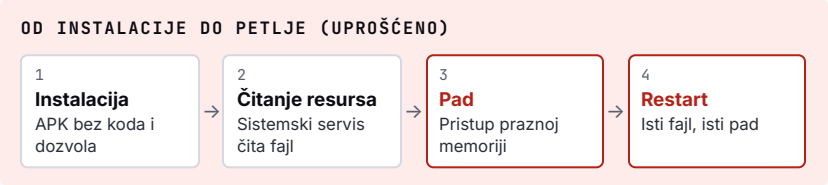
IZVORI

1 **Bitdefender Labs**, GhostMap: The Android flaw that crashes your phone before you open the app, 05.11.2026. bitdefender.com

SECURITY SIGNAL / ANDROID / KAKO RADI

Kada se dva parsera ne slože

Uprošćen prikaz problema, bez detalja koji bi omogućili zloupotrebu.



Otkriće je počelo slučajno. Avgusta je jedan APK sa bankarskim trojancem, prikupljen iz prakse, srušio Bitdefenderove emulatore tokom instalacije. Sve ukazuje na to da autor nije ni znao za taj efekat.

APK je zapravo ZIP arhiva, a svaki unos u njoj navodi način kompresije i veličinu. Android te podatke čita u više biblioteka, i one se ne slažu oko toga šta da provere. Jedna proverava dužinu samo za nekompresovane unose, a druga mapira sve što nije kompresovano na uobičajen način. Unos sa neobičnom oznakom pada baš između ta dva pravila.

Rezultat je da sistem u memoriju mapira mnogo više nego što fajl stvarno sadrži. U testu je APK od nekoliko kilobajta bio mapiran preko oko 16 MB. Kada proces pročita taj prazan deo, kernel ga ubija.

Ako taj proces hostuje većinu Androida, sistem pada, ponovo se diže, ponovo čita isti fajl i ponovo pada. U jednom snimku ciklus se ponovio 110 puta.

Korisniku ostaju ograničene mere: instalirajte aplikacije iz pouzdanih izvora i držite rezervnu kopiju podataka. Bitdefender navodi da njegov mobilni proizvod prepoznaje ovakve fajlove, što je tvrdnja proizvođača.

HRONOLOGIJA

12.08.	Otkrivanje
20.08.	Prva prijava, Won't Fix
25.08.	Druga prijava, van okvira zakrpe
05.11.	**Objava**

IZVORI

1 **Bitdefender Labs**, GhostMap: The Android flaw that crashes your phone before you open the app, 05.11.2026. bitdefender.com

PATCH NOW / 31.10.2026. → 05.11.2026.

Zakrpiti odmah

Stavke koje traže akciju administratora. Prva je potvrđeno iskorišćena, a zakrpa je već dostupna.

WordPress Core pre 7.1.4

CVE-2026-119977

CISA KEV 03.11. | POTVRĐENA EKSPLOATACIJA

Ranjivost u jezgru WordPressa. CISA ju je 3. novembra upisala u katalog aktivno iskorišćenih ranjivosti, a kanadski Centar za sajber bezbednost prenosi upozorenje. To ne znači da su sve instalacije kompromitovane.

ZAKRPA
WordPress 7.1.4, izašao 28. oktobra

ADMIN
Proverite verziju u Dashboardu i da li automatska ažuriranja rade

IZVOR
cyber.gc.ca
wordpress.org

Zyxel GS1900 svičevi

CVE-2026-107441

NAPADI PRIJAVLJENI | LAN, BEZ PRIJAVE

Out-of-bounds write u CGI programu. Napadač sa pristupom lokalnoj mreži može da izvrši OS komande. Detalji na strani 38.

ZAKRPA
2.90 Patch 3

ADMIN
Promenite fabričke lozinke, sklonite upravljanje sa javne mreže

IZVOR
zyxel.com
binarly.io

Better Auth i dodaci

12 upozorenja

1 KRITIČNO | NPM

Koordinisano izdanje za preuzimanje naloga, opoziv sesija i proveru ovlašćenja.

ZAKRPA
1.7.16, 1.8.0-beta.5

ADMIN
Ažurirajte sve pakete zajedno i pročitajte upozorenja za svoje dodatke

IZVOR
better-auth.com
vercel.com

Android 10 i noviji

GhostMap

NEMA ZAKRPE | DOS

Nema zakrpe na dan objave, a napadi nisu viđeni. Oprez sa aplikacijama iz nepoznatih izvora i redovna rezervna kopija.

RIZIK
Gubitak podataka zbog fabričkog resetovanja

IZVOR
bitdefender.com

SECURITY SIGNAL / FRANCUSKA / 2. I 3.11.2026.

Kada sajbernapad promeni temperaturu u frižideru

Napad na dobavljača rashladne opreme pogodio je tri objekta francuske službe za krv. Alarmi i osoblje sprečili su štetu.

U ponedeljak, 2. novembra, u tri objekta francuske službe za transfuziju krvi EFS pragovi temperature i odmrzavanja u rashladnim komorama za plazmu podignuti su na izuzetno visoke vrednosti. Sistemi za nadzor su reagovali, a osoblje je proizvode premestilo ili obezbedilo na vreme.

Prema saopštenju EFS-a od 3. novembra, nijedan krvni proizvod nije izgubljen, nisu utvrđene posledice po zdravlje, a prikupljanje i distribucija nisu prekinuti. Meta napada nije bio sam EFS, nego dobavljač rashladne opreme.

EFS nije imenovao dobavljača. Evropska kompanija Coolworld Rentals potvrdila je incident sa softverom za daljinski nadzor koji je pogodio ograničen broj njenih jedinica i navela da je ranjivost u komponenti treće strane. Francuske vlasti istražuju slučaj, a napadač nije identifikovan.

Nedeljnik Le Canard Enchaîné, koji je prvi objavio priču, navodi da je cilj bio da se temperatura sa minus 30 podigne do 110 stepeni. EFS tu brojku nije potvrdio. Slučaj je stigao posle talasa napada na rashladne sisteme supermarketa u Evropi, ali veza između ta dva događaja nije potvrđena.

PREMA EFS-U

Lokacije
3

Izgubljeni proizvodi
nema

Posledice po zdravlje
nisu utvrđene

Napadač
nije identifikovan

IZVORI

1 **BleepingComputer**, Cyberattack disrupts blood storage refrigeration systems in France, novembar 2026. bleepingcomputer.com

2 **CBS News**, Blood banks hit by cyberattack in France days after European freezer hacks, novembar 2026. cbsnews.com

3 **NBC News**, Cyberattack on French blood bank fridges was thwarted, novembar 2026. nbcnews.com

SECURITY SIGNAL / ANALIZA / ZDRAVSTVO I OT

Alarm koji ne zavisi od napadnutog sistema

Šta bolnice i službe mogu da nauče iz incidenta koji se završio bez štete.

SLOJEVI ZAŠTITE (KONCEPTUALNI PRIKAZ)

Dobavljač	Daljinski pristup uz strogu kontrolu
Mreža	Segmentacija od ostatka ustanove
Uređaj	Fizičke granice koje softver ne može da pomeri
Nadzor	Nezavisni senzori i alarmi
Ljudi	Vežbani plan premeštanja

Ovaj slučaj je koristan upravo zato što se dobro završio. Pokazuje šta je zaštitilo plazmu: nije to bio firewall, nego nezavisan alarm i ljudi koji su znali šta da rade.

Bolnice i službe za krv sve više zavise od dobavljača koji opremu održavaju na daljinu. To je praktično, ali znači da softver koji nikada niste pregledali može da promeni fizičko stanje u vašem magacinu. Rashladna komora je industrijski kontrolni sistem, čak i ako je niko tako ne zove.

Zato se digitalna i fizička bezbednost moraju planirati zajedno. Podešavanje na daljinu treba držati odvojeno od mreže ustanove i ograničiti mu opseg. Ako vrednost od minus 30 stepeni nikada ne sme da pređe određeni prag, ta granica treba da postoji i u samom uređaju, a ne samo u softveru. Nadzor treba da bude nezavisan od kanala kojim stiže komanda, a osoblje treba da ima vežbani plan premeštanja.

Dobavljač je deo vašeg sistema, bez obzira na to šta piše u ugovoru.

IZVORI

1 **BleepingComputer**, Cyberattack disrupts blood storage refrigeration systems in France, novembar 2026. bleepingcomputer.com

2 **CBS News**, Blood banks hit by cyberattack in France days after European freezer hacks, novembar 2026. cbsnews.com

SECURITY SIGNAL / ZYXEL / 03.11.2026.

Zyxel: tri izvora, tri različite stvari

Proizvođač potvrđuje grešku, istraživači vežu napade za nju, a broj uređaja je treća priča.

KO ŠTA TVRDI

IZVOR	TVRDNJA	OCENA
Zyxel	Greška i ispravka, napad sa LAN-a	8,8
Binarly	Uhvaćen exploit gađa ovu grešku	9,8
GreyNoise	996 uređaja, 48 zemalja	procena

Zyxel je 3. novembra objavio upozorenje za CVE-2026-107441, grešku tipa out-of-bounds write u CGI programu firmvera za GS1900 sviče. Napadač bez prijave, sa pristupom lokalnoj mreži, može posebno napravljenim HTTP zahtevom da izvrši komande operativnog sistema. Ispravljene verzije su 2.90 Patch 3, za deset modela, a izašle su još 22. oktobra.

Priča je složenija od upozorenja. GreyNoise je u avgustu izbrojao 996 kompromitovanih GS1900 svičeva u 48 zemalja, od kojih je 564 koristilo fabričke lozinke, i pripisao to starijem propustu CVE-2026-7273. Binarly je potom pokazao da uhvaćeni exploit gađa drugu grešku, a junska zakrpa je nije blokirala.

Zato treba razlikovati izvore. Proizvođač potvrđuje ranjivost i ispravku, a Binarly veže napade za nju. Broj uređaja je procena GreyNoisea. Zyxel ocenjuje grešku sa 8,8 i naglašava lokalnu mrežu, dok Binarly daje 9,8. Nije poznato koji su firmver imali napadnuti uređaji.

Lokalna mreža nije isto što i internet. Ali izložen panel za upravljanje ili kompromitovana radna stanica pretvaraju tu razliku u formalnost. Ažurirajte, promenite fabričke lozinke i sklonite upravljanje sa javne mreže.

BROJKA

996

kompromitovanih uređaja u 48 zemalja, prema GreyNoiseu. Help Net Security

IZVORI

1 **Zyxel**, Security advisory for out-of-bounds write vulnerability in GS1900 series switches, 03.11.2026. zyxel.com

2 **Binarly**, Out-of-bounds write vulnerability in Zyxel GS1900 switches, novembar 2026. binarly.io

3 **Help Net Security**, Patched Zyxel GS1900 switches remained open to in-the-wild exploit, 05.11.2026. helpnetsecurity.com

4 **BleepingComputer**, Zyxel fixes zero-day exploited to hack nearly 1,000 network switches, novembar 2026. bleepingcomputer.com

SECURITY SIGNAL / MSECURE, NIKKE / 3. I 4.11.2026.

Kada je pouzdan izvor problem

Menadžer lozinki bez objašnjenja i zvanični launcher sa tuđim kodom.

MSECURE: UPUTSTVO BEZ OBJAŠNJENJA

Kompanija mSeven je 3. novembra pisala korisnicima menadžera lozinki mSecure da je otkrila „sumnjivu aktivnost“. Preporučila je da odmah zaštite sve što čuvaju: da promene lozinke, ponovo podese dvofaktorsku autentifikaciju i uklone passkeyeve.

Nije rekla šta se dogodilo, kada, ni koliko je korisnika pogođeno. BleepingComputer piše da je haker navodno ukrao šifrovanu bazu, ali to kompanija nije potvrdila. Nema dokaza da su sefovi dešifrovani. Ipak, korisnik mora da radi kao da su podaci izloženi, jer ne zna koji nisu. Kod menadžera lozinki transparentnost je deo bezbednosti.

NIKKE: KOMPROMITOVAN ZVANIČNI KANAL

Shift Up je 4. novembra saopštio da su skripte PC launchera za igru Goddess of Victory: NIKKE možda izmenile treće strane, a klijent je ispravljen istog dana. Prema Kotakuu, kod je 27. septembra ubačen u četiri JavaScript fajla na serverima izdavača Level Infinite, a korišćen je od 30. oktobra. Izdavač potvrđuje da su računari i podaci o nalogu mogli biti izloženi i savetuje da svako ko je od 27. septembra pokretao igru instalira novi klijent sa skenerom. Izvori se razlikuju oko datuma.

Pogođen je PC launcher, ne sve platforme. Pouka je neprijatna: preuzimanje sa zvaničnog kanala više nije isto što i dokaz da je softver bezbedan.

NEPOZNATO

Obim incidenta kod mSecurea nije javno potvrđen, a broj naloga nije objavljen.

IZVORI

1 **The Register**, Password manager mSecure tells users to change passwords, won't say why, 03.11.2026. theregister.com

2 **BleepingComputer**, mSecure password manager hack prompts password reset warnings, novembar 2026. bleepingcomputer.com

3 **Kotaku**, Hugely Popular RPG NIKKE Was Compromised, novembar 2026. kotaku.com

4 **Automaton**, Goddess of Victory: NIKKE PC launcher reportedly compromised in supply-chain attack, novembar 2026. automaton-media.com

SECURITY SIGNAL / OPENAI, DREAMHOST / NOVEMBAR 2026.

Plaćati ljude da nađu ono što modeli propuste

Nagrade rastu, a DreamHost smanjuje procenu obima oktobarskog incidenta.

PRIMER OBRAČUNA IZ OBJAVE OPENAI-JA

OSNOVA	KVALITET	KAMPANJA	LOJALNOST
30.000 $ Kritično, core	→ **× 1,15**	→ **× 1,30**	→ **× 1,15**

OpenAI je 2. novembra povećao nagrade u programu za bezbednosne greške. Sredina raspona za srednje, visoke i kritične nalaze u proseku je više nego četvorostruko veća. Kritična ranjivost u ChatGPT-u, Codexu ili API platformi donosi do 30.000 dolara.

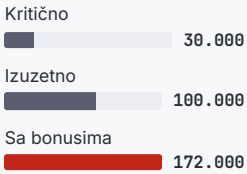
Izuzetni kritični nalazi ostaju na do 100.000 dolara, a uz bonuse za kvalitet, prioritetne kampanje i lojalnost mogu dostići do 172.000 dolara. To je gornja granica koju OpenAI navodi, a ne garantovana isplata. Isti program važi retroaktivno za otvorene prijave.

Poruka je jasna. Kompanija koja sama tvrdi da modeli nalaze hiljade grešaka istovremeno plaća ljude da nađu ono što modeli propuste.

DREAMHOST, NASTAVAK

Incident iz oktobra nije nova priča, ali ima važnu dopunu. Napadač je 23. oktobra otkriven na serveru za File Manager i došao je do FTP i SFTP pristupnih podataka korisnika koji su se tu prijavljivali, kao i do podataka ograničenog broja webmail naloga. Prema DreamHostu, pogođen je deo naloga, znatno ispod približno 10%, što je manje od prve procene. Kompanija nije našla dokaze o pristupu kontrolnom panelu i podacima o plaćanju.

GORNJE GRANICE, USD



Nije garantovana isplata.

IZVORI

1 **OpenAI**, Rewarding defenders with bigger bug bounties, 02.11.2026. openai.com

2 **DreamHost**, October Security Incident, 29.10.2026. dreamhost.com

SECURITY SIGNAL / PREGLED / NOVEMBAR 2026.

Kratki bezbednosni pregled

VREDI ZNATI

TEMA	DATUM	ŠTA JE POTVRĐENO
Google Calendar phishing	04.11.	Material Security opisuje kampanju Operation CloudFire: pozivnice u kalendaru vode na lažne strane preko reverse proxyja, koji preuzima aktivnu sesiju i tako zaobilazi MFA.
GitHub Desktop	02.11.	Dodaje kratkotrajne tokene za autentifikaciju, pa ukraden token duže ne važi.
CodeQL 2.27.4	04.11.	Tačniji upiti i manje lažnih nalaza, posebno kod Jave i Rusta.
Better Auth	03.11.	Dvanaest upozorenja i WAF pravila na Vercelu. Strana 24.
Secret scanning	05.11.	Starlink ključevi i manje lažnih pogodaka. Strana 22.

Pored velikih tema, ove nedelje vredi obratiti pažnju na ono što je manje vidljivo. Kampanja CloudFire je poučna jer pokazuje da MFA ne pomaže kada napadač preuzme već otvorenu sesiju, a Material Security navodi da je blokirao više od 68.000 poruka. Google Kalendar podrazumevano dodaje pozivnice i od nepoznatih pošiljalaca, pa vredi proveriti to podešavanje.

CLOUDFIRE: KADA SU SVI SIGNALI ČISTI

Prema analizi kompanije Material Security, poruke su stizale kao pozivnice za Google Kalendar, često iz organizacije sa kojom je primalac već komunicirao. Povodi su bili obični: govorna pošta, pozivi za ponude, sudski pozivi i neplaćeni računi. Veći deo linkova vodio je na sam Google, pa su domen, sertifikat i reputacija izgledali ispravno.

Napadač je zatim, preko živog reverse proxyja, stajao ispred prave Google strane za prijavu. Žrtva unese lozinku, dobije stvaran zahtev za potvrdu i odobri ga, a napadač dobije sesiju. Zato SMS kodovi i aplikacije za potvrdu ovde ne pomažu. Kampanja traje od sredine avgusta.

ŠTA TO ZNAČI ZA VAS

Administratori treba da prate neobične sesije i nove uređaje, jer napadaču nije potrebno da zna drugi faktor ako preuzme aktivnu sesiju. Korisnicima pomaže ograničenje dodavanja pozivnica od nepoznatih pošiljalaca.

LAB / ANTHROPIC / 02.11.2026.

Može li se matematički dokazati da je AI zaista radio ono što tvrdi?

FlashProve je open source prototip za proverljivu inferenciju. Radi na velikom modelu, ali je i dalje mnogo skuplji od obične obrade.

Kada pitate AI model, ne možete da proverite ko vam je odgovorio. Provajder bi mogao da zameni model jeftinijim, a napadač da podmetne odgovor. Anthropic je 2. novembra objavio FlashProve, open source prototip za proverljivu inferenciju, koji na to pitanje pokušava da odgovori kriptografijom.

Provajder prvo objavi kratku obavezu, otisak tačno određenih težina modela, a težine ostaju tajne. Uz svaki odgovor zatim šalje dokaz koji potvrđuje da te težine, pokrenute na tom promptu, daju tačno te tokene. Reč je o zero-knowledge dokazu: verifikator se uverava da je račun ispravan, a ne saznaje ništa o težinama.

Anthropic je to izmerio na otvorenom modelu Llama 4 Maverick, sa oko 400 milijardi parametara. Jedan H100 GPU pravi dokaze brzinom od oko 110 tokena u sekundi, a dokaz za zahtev od 1.024 tokena ima oko 19 MB. Provera traje oko 17 sekundi na procesoru, bez GPU-a.

Cena je visoka: oko 70 do 95 puta više GPU vremena od obične obrade istog zahteva. Zato je ovo međurezultat i prototip, a ne usluga koja može da se uključi na svim komercijalnim modelima.

BROJKA

19 MB

dokaz za zahtev od 1.024 tokena. Anthropic

BROJKA

70 do 95 ×

više GPU vremena od obične obrade. Anthropic

IZVORI

1 **Anthropic**, Provable inference and FlashProve, 02.11.2026. anthropic.com

LAB / ANTHROPIC / ŠTA SE DOKAZUJE

Dokaz o poreklu nije dokaz o istini

Tačan odgovor i dokazano izvršen račun su dve potpuno različite stvari.

KAKO RADI PROVERA

JEDNOM	→	ZA SVAKI ZAHTEV	→	KOD KORISNIKA
Obaveza		**Dokaz**		**Provera**
Otisak težina, oko 6,5 MB, 39 minuta		Oko 19 MB, na H100 GPU-u		Oko 17 sekundi na CPU-u

ČETIRI RAZLIČITA PITANJA

PITANJE	DA LI FLASHPROVE POMAŽE
Da li je radio deklarisani model?	**Da, u okviru protokola**
Da li dokaz otkriva težine?	Ne, ali arhitektura ostaje poznata
Da li je odgovor tačan?	*Ne, to je van dokaza*

Najvažnije je šta dokaz ne dokazuje. FlashProve potvrđuje da je određeni model izvršio određeni račun. Ne potvrđuje da je odgovor tačan. Model koji halucinira i dalje će halucinirati, samo sa dokazom o poreklu.

Zato treba razlikovati četiri pitanja. Poverenje u provajdera je ono što imamo danas: verujemo da servira ono što tvrdi. Integritet izvršavanja je ono što FlashProve dodaje. Privatnost modela znači da dokaz ne otkriva težine, iako arhitektura ostaje poznata. Kvalitet i istinitost odgovora ostaju van svega toga.

Anthropic navodi nekoliko primena. Regulator bi mogao da proveri da se na hardveru zaista izvršava deklarisani model, a nezavisni ocenjivač da zna da testira isti model koji korisnici dobijaju. Dokaz bi mogao da otkrije i kompromitovan server koji podmeće odgovore.

Sistem je razvijen uz pomoć Claudea, pa je ceo kod otvoren pod licencom Apache 2.0, uz dokaze u formalnom jeziku Lean, da bi ga drugi mogli proveriti. Autori sa Anthropica, EPFL-a i MIT-a pozivaju druge da ga provere i poboljšaju.



LAB / ANTHROPIC / 04.11.2026.

Claude i misterija šupljih čestica

Prva 3D struktura vault čestice iz prokariotskog sveta nije lek, nego nov alat za pitanje staro 40 godina.

Vault čestice su velike šuplje proteinske strukture u obliku bureta, otkrivene 1986. Ima ih u gotovo svim našim ćelijama, a njihova funkcija ni posle 40 godina nije definitivno poznata. Anthropic je 4. novembra objavio prvu trodimenzionalnu strukturu vault čestice iz prokariotskog sveta. Tačnije, protein potiče iz bakteriofaga, virusa koji inficira bakterije, pa se čestica gradi u bakterijskoj ćeliji.

Struktura ima 96 kopija jednog proteina nazvanog L05, naspram 78 u ljudskoj verziji, ukupne mase oko 9,5 megadaltona. Duga je oko 54, a široka oko 45 nanometara.

Claude je radio pod vođstvom naučnika: pretražio je bazu od oko 15 milijardi predviđenih proteina, predlagao DNK konstrukte, optimizovao izolaciju i obradio podatke iz krio-elektronske mikroskopije. Izolacija koja obično traje tri dana skraćena je na oko 90 minuta, a prvi model strukture bio je gotov za 34 sata.

Ovo nije lek ni autonomno otkriće. Funkcija i dalje nije poznata, u džepu proteina stoji neidentifikovan molekul, a Anthropic opisuje i greške: protokol sa pogrešnim dodatkom koštao je tim dve nedelje. Rad je predat kao preprint, a strukture i dodatni podaci stižu kasnije.

UKRATKO

L05
96 kopija proteina

Ljudski vault
78 kopija

Veličina
54 × 45 nm

Izolacija
3 dana na 90 min

STATUS

Funkcija nije poznata. Preprint, bez kliničke primene.

IZVORI

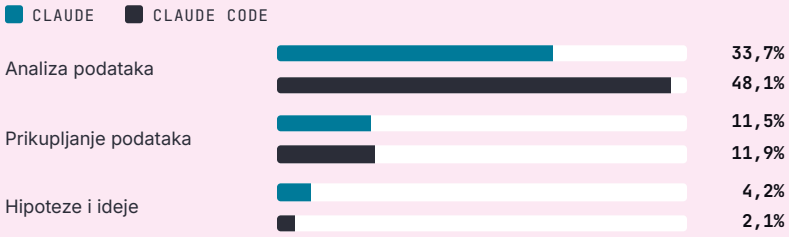
1 **Anthropic**, Investigating vault particles with Claude, 04.11.2026. anthropic.com

LAB / ANTHROPIC / 05.11.2026.

Za šta naučnici zaista koriste Claude

Analiza 207.049 sesija pokazuje da AI najviše radi za tastaturom, a najmanje tamo gde je potrebna laboratorija.

UDEO SESIJA PO TIPU ZADATKA, %



Izabrane kategorije, ne zbir svih. Period 02.08. do 30.09.2026. Izvor: Anthropic.

Anthropic je 5. novembra objavio analizu 207.049 istraživačkih sesija na svojim potrošačkim planovima, u periodu od 2. avgusta do 30. septembra 2026. Od toga je 128.914 iz Claude Chata i Coworka, a 78.135 iz Claude Codea. To su sesije, ne jedinstveni naučnici, i uzorak ne obuhvata druge alate.

Najviše se radi analiza podataka: 33,7% sesija u Claudeu i 48,1% u Claude Codeu, naspram procenjenih 27,6% vremena istraživača. Pisanje i komunikacija čine 32,0% sesija u Claudeu, dvostruko više od njihovog udela u vremenu. Generisanje hipoteza je malo, 4,2% i 2,1%, a prikupljanje podataka 11,5% i 11,9%, iako čini 28,6% istraživačkog vremena.

Računarstvo pravi 32,7% sesija u Claude Codeu, iako ima 4,3% svetskih istraživača. Claude Science, specijalizovani alat, koristi se pre svega u biomedicini i biologiji i za složenije zadatke.

Razlog je očigledan. Ko radi za tastaturom, može da delegira mnogo toga, a pipeta i dalje traži ruku. U laboratorijskim naukama 38 do 41% vremena odlazi na fizičke korake, naspram 4% u prosečnoj oblasti.

UZORAK

Claude
128.914

Claude Code
78.135

Ukupno
207.049

IZVORI

1 **Anthropic**, How researchers use Claude, 05.11.2026.
anthropic.com

LAB / ANTHROPIC / SCENARIJI

Do 15 puta brže, u jednom zamišljenom svetu

Modelovanje nije merenje. Tri scenarija opisuju mogućnosti, ne ostvarenu produktivnost.

SCENARIJI ANTHROPICA

SCENARIO	PRETPOSTAVKA	UBRZANJE
1	Sadašnje mogućnosti, široko usvojene	1,35× do 2,02×
2	AI radi 75% nefizičkih koraka	do oko 8×
3	AI radi sve nefizičke korake	*do 15×, spekulativno*

Nije izmereno povećanje produktivnosti. Izvor: Anthropic.

Anthropic zatim pravi jednostavan model koliko bi AI mogao da ubrza istraživanje. To su scenariji, a ne izmereni rezultati.

U prvom, sadašnje mogućnosti su široko usvojene. AI tada preuzima 27 do 52% vremena potrebnog za novu studiju, a ubrzanje ide od 1,35 puta u umetnosti do oko 2 puta u računarstvu i statistici. U drugom scenariju AI u potpunosti obavlja 75% nefizičkih koraka, pa računarstvo stiže do oko 8 puta. U trećem, potpuno spekulativnom, AI radi sve nefizičke korake i neke oblasti dostižu i do 15 puta, dok laboratorijske nauke ostaju ograničene fizičkim radom.

Dakle, 15 puta nije ostvareno ubrzanje nauke, nego gornja granica jednog zamišljenog sveta. Sam Anthropic ovo opisuje kao istraživanje mogućnosti.

Autori dodaju i anketu 528 naučnika, uglavnom iz biomedicinskih oblasti, koji već aktivno koriste AI. Oko 40% očekuje da će AI samostalno sprovoditi cele projekte do 2030, oko 64% do 2035, a 16% kaže da se to neće desiti. Ti ispitanici su, po izboru, skloniji AI-ju od prosečnog istraživača.

BROJKA

38 do 41 %

vremena u laboratorijskim naukama odlazi na fizičke korake. Anthropic

IZVORI

1 **Anthropic**, How researchers use Claude, 05.11.2026. anthropic.com

LAB / GOOGLE DEEPMIND / 03.11.2026.

Sat vremena hemije, ne sat do leka

Agenti u Antigravityju skraćuju pripremu, ali predlog molekula je tek početak dugog puta.



Google DeepMind je 3. novembra pokazao radni tok koji povezuje agente u okruženju Antigravity sa novim veštinama za hemoinformatiku. Podela posla je važna: jezički model vodi tok rada, pretražuje baze i rezonuje, a deterministične hemijske alatke, zasnovane na otvorenom alatu RDKit, rade proračune. U hemiji greška u jednom atomu daje drugo jedinjenje.

U demonstraciji su polazni primer bili lekovi za rak pluća crizotinib i lorlatinib. Agent je pretražio literaturu, prikupio hiljade jedinjenja, filtrirao nebitne, uporedio srodne parove molekula i predložio nove makrociklične strukture zajedno sa mogućim putevima sinteze. Google navodi da je to trajalo oko sat vremena, dok jedna takva iteracija obično traje više dana.

Treba jasno reći šta to nije. Za sat vremena nije nastao lek. Predlozi su hipoteze iz simulacije. Oni tek treba da se sintetišu, testiraju u laboratoriji i prođu dug put pretkliničkih i kliničkih ispitivanja.

Agent skraćuje pripremu, i to je zaista vredno. Odluku o tome šta vredi napraviti i dalje donosi hemičar.

IZVORI

1 **Google DeepMind**, Agentic cheminformatics with Google Antigravity, 03.11.2026. deepmind.google

LAB / OPENAI / 03.11.2026.

Od CAD modela do stvarnog dela

Modeli pomažu u mašinstvu i elektronici, ali proizvodnja i dalje traži čoveka.

OD MODELA DO PROIZVODA (KONCEPTUALNI PRIKAZ)



OpenAI je 3. novembra opisao kako njegovi modeli pomažu pri projektovanju fizičkih proizvoda: od CAD modela i crteža za proizvodnju do štampanih ploča, simulacija i firmvera.

Najzanimljiviji je test uređaj za razgovor sa Codexom, koji je model GPT-6 Astra projektovao bez direktnih ljudskih izmena, uključujući kućište, ploču i softver. Dva člana tima radila su na tome kao sporedni projekat, kraće od nedelju dana, a mala serija prototipova nastala je za manje od mesec dana.

OpenAI priznaje i ono što nije radilo. Priprema za proizvodnju tražila je više krugova pregleda, jer Astra nije dosledno uzimala u obzir ograničenja proizvođača, tolerancije i detalje montaže.

Chip Ganassi Racing testira pretvaranje 3D skenova starih delova u CAD modele, a inženjeri tima proveravaju rezultate. Sa Mazdom je najavljena nova saradnja na aerodinamici i sudarnoj bezbednosti, a rezultati stižu kasnije. U internom testu BenchCAD 2.0 noviji interni model ima 0,875, naspram 0,594 za Astru, što je tvrdnja proizvođača.

Digitalni model nije proizvod. Materijal, tolerancija i sudar pokazuju se tek na stvarnom delu.

BROJKA

23×

rast upotrebe tokena u hardverskim timovima OpenAI-ja od februara. OpenAI

IZVORI

1 **OpenAI**, Accelerating engineering for the physical world, 03.11.2026. openai.com

MONEY / AMD / 03.11.2026.

AMD: Data Center skoro duplo veći

Rekordan kvartal nosi AI infrastruktura. Rast od 97% odnosi se na jedan segment, a ne na celu kompaniju.

AMD je 3. novembra objavio rekordan kvartal. Prihod je dostigao 13,377 milijardi dolara, 45% više nego godinu dana ranije. Operativni prihod po GAAP-u bio je 2,832 milijarde, a neto dobit 2,428 milijardi.

Pokretač je segment Data Center: 8,5 milijardi dolara, rast od 97%. To je rast tog segmenta, a ne cele kompanije. Razlog su procesori EPYC i početak isporuka GPU serije Instinct MI450. AMD navodi da Anthropic, Meta, Microsoft, OpenAI i Oracle već pokreću modele na prvim rack sistemima Helios.

Slika nije ista svuda. Client i Gaming zajedno su pali za 8%, na 3,7 milijardi. Client je porastao 7%, a Gaming je pao 40%, na 773 miliona. Embedded je porastao 29%, na 1,1 milijardu.

Za četvrti kvartal kompanija očekuje oko 17 milijardi dolara, uz moguće odstupanje od 3%. To bi bio rast od oko 66%.

NVIDIA ostaje vodeća na tržištu AI ubrzivača. Brz rast sa manje osnove pokazuje da AMD uzima značajan deo novog posla, ali sam po sebi ne dokazuje promenu lidera.

BROJKA

8,5 mlrd $

prihod Data Center segmenta, rast 97%. AMD

Q3 2026

Prihod
13,377 mlrd $

Rast
45%

Op. prihod
2,832 mlrd $

Neto
2,428 mlrd $

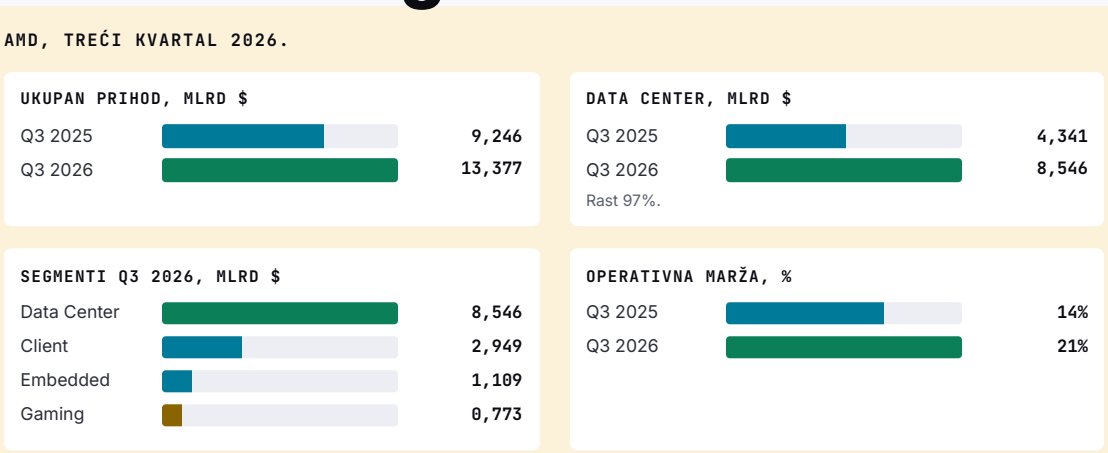
IZVORI

1 **AMD**, AMD Reports Third Quarter 2026 Financial Results, 03.11.2026. newsroom.amd.com

MONEY / AMD / INFOGRAFIKA

AMD u četiri grafikona

AMD, TREĆI KVARTAL 2026.



Podaci po GAAP-u. Izvor: AMD.

SEGMENTI, MILIONI DOLARA

SEGMENT	Q3 2025	Q3 2026	PROMENA
Data Center	4.341	**8.546**	+97%
Client	2.750	2.949	+7%
Gaming	1.298	773	*minus 40%*
Embedded	857	1.109	+29%

Grafikoni ispod koriste podatke iz AMD-ovog izveštaja za treći kvartal 2026. Operativna marža je porasla sa 14% na 21%, jer su prihodi rasli brže od troškova poslovanja. Data Center sada čini oko 64% ukupnog prihoda, naspram oko 47% pre godinu dana.

ŠTA GRAFIKONI POKAZUJU

Gaming je jedini segment u padu, sa 1,298 na 0,773 milijarde dolara, pa je AMD danas mnogo manje zavisan od ciklusa konzola i grafičkih kartica. Client je porastao zahvaljujući mobilnim Ryzen procesorima.

Data Center je istovremeno najprofitabilniji segment u apsolutnom iznosu, sa 2,882 milijarde operativnog prihoda, naspram 1,074 milijarde godinu dana ranije. Lisa Su kaže da je prihod premašio gornju granicu prognoze i da potražnja za proizvodima Instinct i EPYC jača.

Prognoza za četvrti kvartal, oko 17 milijardi dolara, znači rast od oko 27% u odnosu na treći kvartal. To je očekivanje kompanije, a ne ostvaren rezultat, i zavisi od toga koliko brzo sistemi Helios prelaze iz prvih instalacija u velike isporuke.

MONEY / APPLE / 02.11.2026.

Apple: rekord bez AI priče u brojkama

Kvartalni prihod od 114,5 milijardi dolara. Treba razlikovati kvartal i fiskalnu godinu.

KVARTAL I FISKALNA GODINA

POKAZATELJ	VREDNOST	PERIOD
Prihod	114,5 mlrd $	FQ4, do 26.09.
Bruto marža	47,9%	FQ4
Zarada po akciji	2,10 $	FQ4
Prihod	479 mlrd $	Fiskalna 2026.

Apple je 2. novembra objavio rezultate za četvrti fiskalni kvartal, završen 26. septembra. Prihod je 114,5 milijardi dolara, 12% više nego godinu ranije, što je rekord za septembarski kvartal. Bruto marža je 47,9%, a zarada po akciji 2,10 dolara, uz pozitivan uticaj povraćaja carina, oko jedan procentni poen na maržu i 5 centi na zaradu.

Treba razlikovati kvartal i godinu. Cela fiskalna 2026. donela je rekordnih 479 milijardi dolara. Direktor John Ternus navodi rekord iPhonea za septembarski kvartal i najveći prihod od usluga do sada.

Apple u saopštenju ističe nove uređaje, među njima iPhone Duo i iPhone 18 Pro, a novi MacBook Pro sa ekranom na dodir iz prošlog broja počinje da stiže kupcima 6. novembra. Iz samog izveštaja ne može se izdvojiti koliko su rastu doprinele AI funkcije.

Apple je u ovoj priči suprotnost AMD-u. Ne prodaje ašove za AI groznicu, nego uređaje na kojima se AI koristi, a zarada ostaje vezana za telefon i usluge.

BROJKA

114,5 mlrd $

prihod u kvartalu, rast 12%. Apple

BROJKA

479 mlrd $

prihod cele fiskalne 2026.. Apple

IZVORI

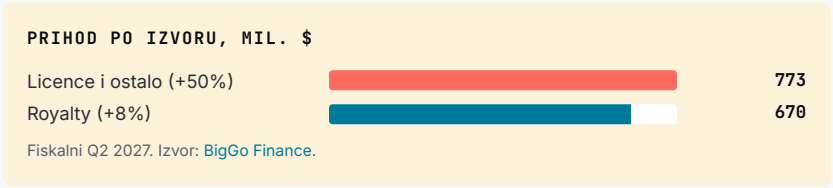
1 **Apple**, Apple reports fourth quarter results, 02.11.2026. apple.com

2 **Apple**, Apple unveils groundbreaking MacBook Pro with PROLED XDR display, 28.10.2026. apple.com

MONEY / ARM / 04.11.2026.

Arm prodaje nacrte, a sada i više od toga

Prihod raste 27%, ali licence rastu mnogo brže od royaltyja.



Arm je 4. novembra prijavio prihod od oko 1,44 milijarde dolara za drugi fiskalni kvartal 2027, 27% više nego godinu dana ranije. Rast ne dolazi ravnomerno. Prihod od licenci i ostalog skočio je 50%, na 773 miliona, dok je royalty porastao 8%, na 670 miliona.

Za razumevanje Arma ta razlika je ključna. Kompanija tradicionalno ne proizvodi čipove, nego prodaje intelektualnu svojinu. Licenca se plaća za pristup arhitekturi, a royalty za svaki proizvedeni čip. Licenca zato pokazuje šta se sprema, a royalty šta se trenutno prodaje.

Uprava navodi da je royalty iz data centara udvostručen, dok su telefoni pod pritiskom cena memorije. Velike cloud kompanije prave sopstvene serverske procesore na Arm osnovi, pa Arm zarađuje i kada nijedan njegov čip ne stoji na polici.

Kompanija sada i sama razvija silicijum: očekivanja za AGI CPU podignuta su na do 2 milijarde dolara prihoda u dve fiskalne godine. To je pomeranje od prodavca nacrta ka prodavcu proizvoda. Izvori ovde su transkript i sažeci poziva sa investitorima.

IZVORI

1 **The Motley Fool**, Arm Holdings Q2 2027 earnings call transcript, 05.11.2026. fool.com

2 **BigGo Finance**, Arm Holdings Q2 2027 earnings call summary, 04.11.2026. finance.biggo.com

INFRA / TERAWULF, GOOGLE, ANTHROPIC / 04.11.2026.

Kako izgleda garancija od 401 megavat

Google daje kreditnu podršku za Anthropicov zakup kod kompanije TeraWulf. Kapacitet je planiran, ne operativan.

KO KOME GARANTUJE (UPROŠĆENO)



TeraWulf je 4. novembra saopštio da je dobio kreditnu podršku Googlea za projekat u Hawesvilleu, u američkoj državi Kentucky. Kampus se gradi za Anthropic, na osnovu 20-godišnjeg zakupa potpisanog u julu, vrednog oko 19 milijardi dolara. Planirani kapacitet je oko 401 megavat kritičnog IT opterećenja, a to je projekat, ne operativni kapacitet. Prvi kapaciteti očekuju se u drugoj polovini 2027.

Sporazum je najzanimljiviji po onome što otkriva o finansiranju. TeraWulf prelazi sa rudarenja bitcoina na AI infrastrukturu i nema kreditni rejting velike tehnološke kompanije. Sa garancijom Googlea, zajmodavci vide drugačiji rizik, pa se dug može dobiti pod boljim uslovima. Prema izveštajima o podnesku, Google u slučaju problema može da preuzme zakup ili plati naknadu, što može da mu donese udeo u projektnoj kompaniji.

To je jedan veliki partner koji jemči za zakup svog partnera, a Google je i ulagač u Anthropic. Isti novac sve češće kruži između čipa, zakupa i modela.

PROJEKAT

Lokacija
Hawesville, Kentucky

Kapacitet
oko 401 MW, plan

Zakup
20 godina

Vrednost
oko 19 mlrd $

Prvi kapacitet
druga polovina 2027.

IZVORI

1 **Reuters preko KFGO**, TeraWulf gets credit backstop from Google for Anthropic data-center project, 04.11.2026. kfgo.com

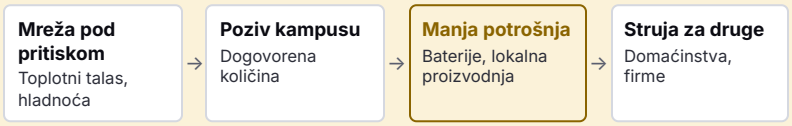
2 **CoinDesk**, Google could take ownership stake in TeraWulf's AI project if Anthropic defaults, 05.11.2026. coindesk.com

INFRA / OPENAI / 02.11.2026.

Računarski kampus kao rezerva za mrežu

Grid Protectors je program, a ne izgrađen kapacitet.

KAKO BI TO RADILO (KONCEPTUALNI PRIKAZ)



OpenAI je 2. novembra pokrenuo program Grid Protectors, saradnju sa komunalnim preduzećima, regulatorima i donosiocima odluka u SAD. Ideja je da budući računarski kampusi smanje potrošnju kada je mreža pod opterećenjem, a da komunalne službe tu fleksibilnost mogu da koriste kao resurs.

Prvi primer je planirani kampus u okrugu Effingham u Džordžiji, koji je još u razvoju i služiće kao pilot. Ugovor sa kompanijom Georgia Power obuhvata do 1.000 megavata fleksibilne potrošnje, što OpenAI poredi sa prosečnom potrošnjom oko 700.000 domaćinstava.

OpenAI obećava da će sam plaćati svoje troškove struje i infrastrukture i tvrdi da stalna potrošnja može da pomogne da se fiksni troškovi mreže rasporede na više korisnika. Porodice i mala preduzeća, kaže kompanija, ne treba da subvencionišu kampus.

To je program, a ne izgrađen kapacitet. Uslovi će se razlikovati po lokacijama, a kompanija navodi da će dodatne obaveze objaviti kada budu dogovorene. Hoće li se račun lokalnih korisnika zaista smanjiti ili bar ostati isti, pokazaće tek stvarne cene.

BROJKA

1.000 MW

fleksibilne potrošnje u ugovoru sa kompanijom Georgia Power. OpenAI

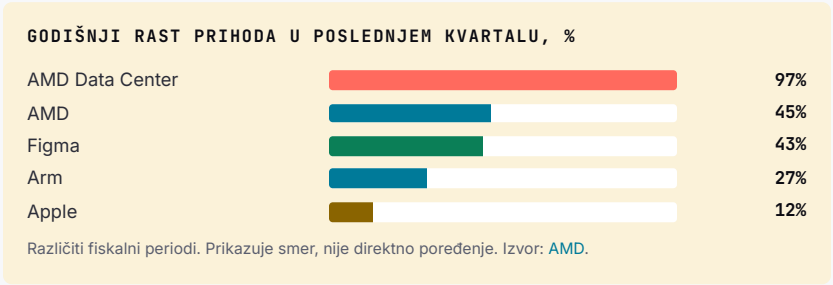
IZVORI

1 **OpenAI**, Grid Protectors Program, 02.11.2026. openai.com

MONEY / FIGMA / 04.11.2026.

Ko zarađuje u ovoj fazi

Kratak pogled na manji izveštaj i šta on dodaje velikoj slici.



Pored velikih izveštaja, nekoliko manjih brojki govori istu priču iz drugog ugla.

Figma je 4. novembra objavila prihod od 391,4 miliona dolara za treći kvartal, što je rast od 43%. Po GAAP-u kompanija je u gubitku iz poslovanja od 119,2 miliona, a bez stavki koje se isključuju ima 47 miliona dobiti. Za celu godinu očekuje prihod od 1,497 do 1,499 milijardi dolara.

Rast tu nosi softver koji koristi AI, ali trošak AI-ja je sada stavka koju investitori posebno prate. Isti pritisak vidi se kod svih koji AI nude uz pretplatu.

Između Figme, Arma i AMD-a vidi se raspored ove faze. Najbolje prolaze oni koji prodaju kapacitet i arhitekturu za izgradnju. Aplikativni softver raste, ali mora da dokaže da može i da zaradi.

Rast u grafikonu nije direktno uporediv, jer su periodi i veličine kompanija različiti. Koristan je samo kao pokazatelj smera: najbrže rastu oni koji su najbliži infrastrukturi ili proizvodu koji se prodaje uz AI.

BROJKA

391,4 mil.

$

prihod Figme u Q3, rast 43%. Figma

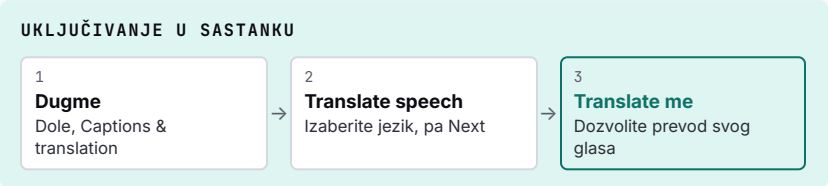
IZVORI

1 **Figma**, Figma Announces Third Quarter 2026 Financial Results, 04.11.2026. investor.figma.com

WORK / GOOGLE MEET / VODIČ

Kako uključiti prevođenje u Google Meetu

Tri koraka, prema zvaničnoj dokumentaciji.



WHATSAPP DOGAĐAJI IZLAZE IZ GRUPE

Meta je 5. novembra proširila funkciju Events. Nova strana Events Home, u podešavanjima, okuplja prošle i buduće događaje. Pozivnica se može poslati linkom i osobama bez naloga, koje vide detalje i potvrđuju dolazak bez instaliranja aplikacije. Dodati su podsetnici i pratilac. Vaš broj nije vidljiv gostima koje ne poznajete, a gosti bez naloga adresu vide tek posle potvrde. Uvođenje traje narednih nedelja, pa funkcija neće svima stići odjednom.

FITBIT EDGE

Google je izbacio Fitbit Edge, narukvicu koja zamenjuje model Charge 6. Prema dostupnim izveštajima, cena je 179,99 dolara, a u prodaji je od 27. oktobra. Ima AMOLED ekran od 1,34 inča, EKG, merenje kiseonika i do sedam dana baterije, ali nema NFC za plaćanje.

UČENJE UMESTO GOTOVOG ODGOVORA

Google je 3. novembra proširio Guided Learning u Classroomu, gde postaje podrazumevani chatbot, a nastavnici mogu da vide razgovore. Režim vodi učenika kroz zadatak umesto da daje rešenje. U Pretrazi je najavljen pilot u izabranim američkim školama. Škole će, prema najavi, morati same da uključe Gemini za učenike K-12 uzrasta.

IZVORI

1 **Google Meet Help**, Use Speech Translation, novembar 2026. support.google.com

2 **Meta**, WhatsApp Events brings people together beyond the group chat, 05.11.2026. about.fb.com

3 **Android Authority**, Google Fitbit Edge launches with 7-day battery for $180, oktobar 2026. androidauthority.com

4 **Google**, Responsible AI for schools with Guided Learning, 03.11.2026. blog.google



Ilustracija: trag povratka kroz atmosferu i daleki gama bljesak. 0000000, NIJE FOTOGRAFIJA

ORBIT / NASA / 04.11.2026.

Swift je završio misiju

Opservatorija predviđena za dve godine radila je skoro 22, a povratak u atmosferu potvrđen je 4. novembra iznad Sumatre.

Posle skoro 22 godine u orbiti, NASA-ina opservatorija Neil Gehrels Swift ušla je u Zemljinu atmosferu 4. novembra, u 12:39 UTC, iznad severne Sumatre. Svemirske snage SAD potvrdile su povratak na oko 3,4 stepena severne širine i 98,6 stepeni istočne dužine. Očekivalo se da većina letelice izgori, a neki delovi su možda preživeli.

Swift je lansiran 2004, sa planom za dvogodišnju osnovnu misiju. Trebalo je da lovi gama bljeskove, najsnažnije eksplozije u kosmosu. Tri teleskopa, za gama, rendgensko i ultraljubičasto i optičko zračenje, omogućila su mu da se brzo okrene ka izvoru i pošalje upozorenje drugim opservatorijama.

Tokom decenija Swift je postao univerzalan alat astronoma, od aktivnih galaksija do kometa u našem sistemu.

Kraj je došao zbog otpora atmosfere, koji je pojačala sunčeva aktivnost. Komercijalna misija koja je trebalo da podigne orbitu završena je u avgustu bez pokušaja. Dvadesetog oktobra, na visini od 275 kilometara, tim sa Penn Statea poslao je poslednju komandu i završio rad.

SWIFT

Lansiran
2004.

Plan
2 godine

Povratak
04.11. 12:39 UTC

Mesto
Severna Sumatra

IZVORI

1 **NASA**, NASA's Swift Observatory Re-Entered Atmosphere, 04.11.2026. science.nasa.gov

2 **NASA**, NASA's Swift Mission Ends Ahead of Re-Entry, 23.10.2026. science.nasa.gov

ORBIT / NASA / 2004 → 2026

Dvadeset dve godine u jednoj liniji

Vremenska linija misije i neuspeli pokušaj spasavanja.

MISIJA SWIFT

2004	avg. 2026.	sept. 2026.	20.10.	04.11.
Lansiranje	**Servis otkazan**	**Nazad na nauku**	**275 km**	**Povratak**
Plan: dve godine	Bez pokušaja podizanja	Stotine meta	Kraj rada	12:39 UTC

Priča o Swiftu ima i poslovnu stranu. U 2026. NASA je pokušala nešto neobično: da komercijalna letelica pristupi opservatoriji i podigne joj orbitu. Da bi kupio vreme, tim je obustavio naučna posmatranja kako bi se smanjio otpor.

Misija je u avgustu završena bez pokušaja podizanja. Swift se zatim vratio nauci i uspeo da posmatra još stotine meta, od ostataka eksplozija zvezda do kometa. Taj rad je povećao otpor, pa je letelica ponovo počela brzo da pada.

Za svemirske teleskope ovo je pouka o tome koliko su dugovečne misije zavisne od stvari koje se ne vide na početku. Letelica predviđena za dve godine radila je jedanaest puta duže, a završila je zbog Sunca, ne kvara.

ŠTA OSTAJE IZA SWIFTA

Tri instrumenta bila su osmišljena da rade zajedno. Letelica posle otkrivanja bljeska sama se okreće ka izvoru, a ostali teleskopi snimaju ono što ostaje. Takav rad, sa upozorenjem drugim opservatorijama u istom trenutku, bio je i ostao model za praćenje kratkotrajnih događaja na nebu.

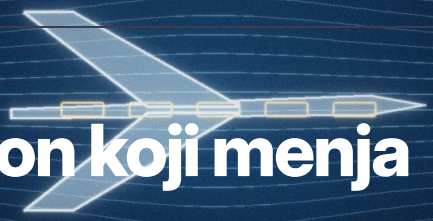
IZVORI

1 **NASA**, NASA's Swift Mission Ends Ahead of Re-Entry, 23.10.2026. science.nasa.gov

2 **NASA**, NASA's Swift Observatory Re-Entered Atmosphere, 04.11.2026. science.nasa.gov

ORBIT / NASA / 04.11.2026.

X-70 Fractal: avion koji menja opremu



NASA je predstavila modularnu platformu za istraživanje leta. Prvi let pod NASA-inom oznakom očekuje se u naredne dve godine.

NASA je 4. novembra, na skupu UP.Summit u Kennedy svemirskom centru, predstavila eksperimentalni avion X-70 Fractal. To je istraživačka platforma sa posadom, namenjena razvoju i testiranju naprednih tehnologija upravljanja letom i upravljivosti.

Ključna reč je modularnost. Avion nosi do oko 907 kilograma eksperimentalne opreme, u unutrašnjim i spoljnim pozicijama, a oprema se može brzo menjati. Tako jedan avion može da služi za niz različitih eksperimenata, umesto da se za svaki gradi nova letelica. Upravljanje se može brzo rekonfigurisati, što NASA-i daje mogućnost da ispita upravljivost na načine koji do sada nisu probani u letu sa posadom.

Prema NASA-i, poletna masa je oko 4.536 kilograma, krstarenje na 0,75 maha, plafon do oko 13.700 metara, a dolet preko oko 2.780 kilometara.

Avion još nije leteo pod NASA-inom oznakom. Administrator Jared Isaacman očekuje prvi let u naredne dve godine. Slika koju je NASA objavila je generisana, a ilustracija na ovoj strani je naša i ne prikazuje stvaran izgled.

X-70

Oprema
do oko 907 kg

Masa
oko 4.536 kg

Brzina
0,75 maha

Status
još nije leteo za NASA-u

IZVORI

1 **NASA**, NASA Announces X-70 Experimental Aircraft to Advance Flight Research, 04.11.2026. nasa.gov

ORBIT / NASA, ESA / NOVEMBAR 2026.

Dva preleta, jedna fotografija, jedno sletanje

Šta sledi u svemiru, sa jasnom razlikom između plana i završenog.

PLANIRANA PUTANJA ESCAPADE (KONCEPTUALNI PRIKAZ)

07.11.	09.11.	10 meseci	sept. 2027.
Prva letelica Motorni prelet	**Druga letelica** Motorni prelet	**Krstarenje**	**Mars** 7. i 9. septembar

NEXT: ESCAPADE KREĆE KA MARSU

Dve NASA-ine letelice ESCAPADE izvešće manevar koji agencija nije izvodila: motorni prelet Zemlje. Prva oko 5:00 EST u subotu, 7. novembra, a druga oko 6:00 EST u ponedeljak, 9. novembra. U najbližoj tački svaka će pali motor oko 9 minuta, pa će joj brzina porasti sa oko 6,3 na oko 6,7 milja u sekundi.

U trenutku izlaska ovog broja manevri se još nisu dogodili. Ako prođu po planu, sledi 10 meseci krstarenja i dolazak na Mars 7. i 9. septembra 2027. Letelice će proučavati kako Sunčev vetar utiče na atmosferu planete.

HERA STIŽE DO DIDIMOSA

Evropska sonda Hera je 18. oktobra, sa oko 1.280 kilometara, prvi put razdvojila Didimos i Dimorfos. Dimorfos je tada bio tačka široka oko piksel. Prema izveštajima, ESA je najavila detaljnije fotografije za 25. novembar. One još nisu objavljene.

SPLICE BIRA GDE DA SLETI

NASA je objavila rezultate testa sistema SPLICE, izvedenog 27. avgusta sa dronom Alta-X u Kaliforniji. Sistem tokom spuštanja lidarom mapira teren, procenjuje opasnosti i preusmerava letelicu na bezbednije mesto. Test je iz avgusta, a objava iz novembra.

IZVORI

1 **NASA**, NASA's Twin ESCAPADE Spacecraft to Slingshot Past Earth on Way to Mars, 02.11.2026. science.nasa.gov

2 **Space.com**, Dimorphos in sight: Europe's Hera probe gets its 1st look at battered space rock, novembar 2026. space.com

3 **NASA**, Safe and Precise Landing, Integrated Capabilities Evolution, 2026. nasa.gov

USE THIS / GITHUB ACTIONS / 02.11.2026.

Proverite svoje workflowe pre 9. novembra

GitHub menja podrazumevano pravilo za pull_request_target u javnim repozitorijumima. Vodič u šest koraka.

GitHub će od 2. decembra podrazumevano blokirati događaj pull_request_target u svim javnim repozitorijumima, osim ako ga primenljiva politika izričito dozvoljava. Promena je pomerena sa 2. novembra. Pre toga stižu dve probe. Ako workflow zavisi od ovog okidača, prvi put će se videti u ponedeljak, 9. novembra.

KOGA SE TIČE

Javnih repozitorijuma na planovima Free, Team i Enterprise Cloud. Privatni i interni repozitorijumi nisu obuhvaćeni, kao ni GitHub Enterprise Server.

ŠTA JE PULL_REQUEST_TARGET

Običan pull_request iz forka radi bez tajni i sa ograničenim tokenom. Događaj pull_request_target radi u kontekstu osnovnog repozitorijuma i može da pristupi tajnama. To je korisno za oznake i komentare. Opasno je kada takav workflow preuzme i pokrene kod iz forka, jer tada nepoznat kod dobija vaše tajne.

KORAK 1: PRONAĐITE UPOTREBU

U pretrazi koda na GitHubu ograničite putanju na .github/workflows i tražite pull_request_target. Lokalno je dovoljno pretražiti isti folder. Proverite i pozive deljenih workflowa.

KORAK 2: POGLEDAJTE INSIGHTS

Pravilo trenutno radi u evaluate režimu, u kome se workflowi izvršavaju, a sistem beleži šta bi bilo blokirano. U Insights delu politika za Actions vidite runove koji bi pali. To je najpouzdaniji spisak, jer pokazuje stvarnu upotrebu.

DATUMI

09.11.	Proba 16 do 18 UTC
16.11.	Proba 16 do 18 UTC
02.12.	Trajno blokiranje

IZVORI

1 **GitHub**, pull_request_target blocked by default December 2, 02.11.2026. github.blog

2 **GitHub Docs**, Governing execution of GitHub Actions workflows, 2026. docs.github.com

USE THIS / GITHUB ACTIONS / KORACI 3 DO 6

Ne ukidajte zaštitu zbog jednog workflowa

Najbolje rešenje je da workflow prestane da treba opasan okidač.

KORAK 3: PROCENITE SVAKI WORKFLOW

Za svaki pronađeni workflow odgovorite na tri pitanja. Da li mu zaista trebaju tajne ili token sa pravom pisanja? Da li preuzima kod iz pull requesta i izvršava ga, uključujući instalaciju zavisnosti i build skripte? Ko sme da ga pokrene?

Ako ne treba poseban pristup, pređite na pull_request. To je najčistije rešenje. Ako vam treba samo označavanje ili komentar, workflow ne sme da pokreće kod iz forka. Težak posao možete da odvojite: nepouzdan deo radi u pull_request bez tajni, a rezultat obrađuje poseban korak.

KORAK 4: USKO IZUZEĆE, SAMO AKO MORA

Ako je okidač opravdan, dozvolite ga u primenljivoj Actions event politici i koristite ciljanje po workflow fajlu, tako da izuzeće važi samo za te fajlove. Ne isključujte zaštitu za celu organizaciju da biste spasli jedan workflow.

KORAK 5: ZAPIŠITE ODLUKU

Uz svako izuzeće zapišite koji fajl je u pitanju, zašto mu treba okidač, ko je odobrio i kada se ponovo proverava. Kada se zaštita ukine bez razloga, šteta se ne vidi sve do incidenta.

KORAK 6: ISKORISTITE PROBE

Tokom proba blokirani pokušaji prave neuspele runove sa porukom o grešci, a workflow se ne izvršava. Posle prozora sistem se vraća na evaluate režim. Probu na vreme najavite timu i pratite pull requestove iz forkova u tom periodu.

PRAVILO

Workflow sa tajnama ne sme da preuzima, gradi ni pokreće kod iz nepouzdanog pull requesta.

IZVORI

1 **GitHub Docs**, Securely using pull_request_target, 2026. docs.github.com

2 **GitHub Docs**, Governing execution of GitHub Actions workflows, 2026. docs.github.com

SHIPPED / 31.10.2026. → 05.11.2026.

Stiglo ove nedelje

Šta je zaista dostupno, sa platformom i ograničenjem. Najavljena kupovina Pierrea i planovi nisu na ovoj strani.

OPENAI · 04.11.

Images 2.6

ChatGPT, Codex i API, svi planovi. Šest sekundi nije garantovano vreme.

DOSTUPNO OpenAI

GITHUB · 04.11.

Copilot u Xcodeu

Od Xcode 27.3 beta, Mac sa macOS Tahoe 26.6. Odvojeno od ekstenzije.

PUBLIC PREVIEW GitHub

VERCEL · 03.11.

Security Review

Pro i Enterprise. Besplatno do 10. novembra. Nije bezbednosna revizija.

BETA Vercel

VERCEL · 02.11.

vercel.toml

Svi projekti. Samo jedan konfiguracioni fajl po projektu.

DOSTUPNO Vercel

VERCEL · 03.11.

vercel doctor

CLI provera podešavanja. Dijagnostika, ne ispravlja sama.

DOSTUPNO Vercel

GITHUB · 05.11.

Secret scanning detektori

Starlink ključevi i manje lažnih pogodaka. Partnerski tok važi za javne repozitorijume.

DOSTUPNO GitHub

META · 05.11.

Muse Voice

Mobilni, web i Mac, ali za početak samo SAD.

ROLLOUT Meta

META · 05.11.

WhatsApp Events

Stiže tokom narednih nedelja, ne svima odjednom.

ROLLOUT Meta

GOOGLE · 02.11.

Meet, 63 jezika

Web, Android i iOS, uz odgovarajući plan. Regionalna ograničenja.

ROLLOUT Google Workspace Updates

VERCEL · 04.11.

Kimi K3.1 ZDR

Više provajdera bez čuvanja podataka preko AI Gatewaya.

DOSTUPNO Vercel

5 MINUTES / 31.10.2026. → 05.11.2026.

Ukratko

Kratke vesti. Ako je tema obrađena u članku, kartica vodi na njega.

GITHUB · 04.11.

CodeQL 2.27.4

Tačniji upiti za Javu, Rust i C++, kao i jače provere pri objavljivanju paketa. Strana 22.

GitHub

GITHUB · 03.11.

BYOK usage API

Upotreba sopstvenih ključeva vidi se odvojeno. Strana 21.

GitHub

GITHUB · 03.11.

Dependabot APM

Veštine i instrukcije agenata dobijaju ažuriranja verzija. Strana 21.

GitHub

VERCEL · 04.11.

Workflow SDK

Duplirani start sa istim tokenom više ne pravi novi run.

Vercel

VERCEL · 03.11.

Vercel CI

Radi i bez povezanog Vercel projekta.

Vercel

GOOGLE · 05.11.

Skica u aplikaciju

Fotografija crteža postaje interaktivni prototip. Strana 32.

Google

GOOGLE · 10.2026

Fitbit Edge

Narukvica od 179,99 dolara, bez NFC-a. Strana 56.

Android Authority

OPENAI · 02.11.

LifeVal

Test za svakodnevne zadatke, autor je sam proizvođač. Strana 32.

OpenAI

OPENAI · 02.11.

Bug bounty

Do 30.000 dolara osnovno, sa bonusima do 172.000. Strana 40.

OpenAI

META · 05.11.

WhatsApp Events

Pozivnice i za ljude bez naloga. Strana 56.

Meta

THIS WEEK IN NUMBERS / 31.10.2026. → 05.11.2026.

Nedelja u brojkama

948

radnih exploita za lokalnu eskalaciju u Linuxu, u istraživanju OpenAI-ja

OPENAI · 04.11.

81

nova ranjivost visoke ozbiljnosti u Firefoxu

OPENAI · 05.11.

1.724

reprodukovane Linux ranjivosti

OPENAI · 04.11.

2.308

kandidata u prolazu, što nisu potvrđeni napadi

OPENAI · 04.11.

48,5%

GPT-6 Cyber na testu ExploitGym, tvrdnja proizvođača

OPENAI · 05.11.

1,2 mil. $

API trošak opisanog Linux prolaza

OPENAI · 04.11.

63

jezika za govorno prevođenje u Meetu

GOOGLE WORKSPACE UPDATES · 22.10.

50%

brže generisanje, prema OpenAI-ju za Images 2.6

OPENAI · 04.11.

THIS WEEK IN NUMBERS / 31.10.2026. → 05.11.2026.

Još brojki nedelje

19 MB

FlashProve dokaz za zahtev od 1.024 tokena

ANTHROPIC · 02.11.

207.049

istraživačkih sesija, što nije broj naučnika

ANTHROPIC · 05.11.

8,5 mlrd $

prihod AMD Data Center segmenta

AMD · Q3

97 %

godišnji rast tog segmenta, ne cele kompanije

AMD · Q3

114,5 mlrd

dolara, Apple, prihod u kvartalu

APPLE · FQ4

1,44 mlrd $

Arm, prihod u kvartalu

THE MOTLEY FOOL · FQ2

skoro 22 godine

trajanje misije Swift, planirano dve

NASA · 04.11.

12

Better Auth bezbednosnih upozorenja

BETTER AUTH · 03.11.

NEXT / 31.10.2026. → 05.11.2026.

Šta pratimo

Budući događaji posle preseka 5. novembra. Nijedan od njih se u trenutku zaključenja još nije dogodio.

→ 06.11.

MacBook Pro

Prema Appleovom rasporedu, novi model počinje da stiže kupcima.

Apple

→ 07.11.

ESCAPADE, prvi prelet

Oko 5:00 EST, motorni prelet Zemlje.

NASA

→ 09.11.

ESCAPADE, drugi prelet

Oko 6:00 EST, druga letelica.

NASA

→ 09.11.

GitHub Actions, prva proba

Od 16 do 18 UTC u javnim repozitorijumima.

GitHub

→ 13.11.

Conductor Cloud

Prelazi u režim samo za čitanje.

Conductor

→ 16.11.

GitHub Actions, druga proba

Isti prozor, od 16 do 18 UTC.

GitHub

→ 18.11.

Voyager 1

Planirana prekretnica: jedan svetlosni dan od Zemlje.

NASA

→ 20.11.

Conductor Cloud

Potpuno gašenje i početak brisanja podataka.

Conductor

→ 25.11.

ESA Hera

Najavljene detaljnije fotografije Didimosa i Dimorfosa.

Space.com

→ 02.12.

pull_request_target

Trajno podrazumevano blokiranje u javnim repozitorijumima.

GitHub

IZVORI / 31.10.2026. → 05.11.2026.

Svi izvori broja

Izvori su grupisani po stranama, redom kojim se prvi put pojavljuju. Primarni izvor ide prvi. Svaki link je aktivan.

06 TEMA BROJA: KOD JE POSTAO INFRASTRUKTURA

1. **Anthropic**. Redesigning source control at Anthropic. 13.10.2026. anthropic.com/engineering/redesigning-source-control
2. **OpenAI**. Scaling Git at OpenAI. 02.11.2026. openai.com/index/scaling-git-at-openai/
3. **OpenAI**. A thousand fewer paths to root. 04.11.2026. openai.com/index/a-thousand-fewer-paths-to-root/

07 TEMA BROJA: KONTROLA JE POSTALA GLAVNI TROŠAK

4. **OpenAI**. GPT-6 Cyber: Advancing the frontier of aligned cybersecurity agents. 05.11.2026. openai.com/index/introducing-gpt-6-cyber/
5. **Anthropic**. Provable inference and FlashProve. 02.11.2026. anthropic.com/research/provable-inference

08 SECURITY: AI JE UŠAO U NOVU FAZU SAJBERBEZBEDNOSTI

6. **OpenAI**. GPT-6 Cyber System Card. 05.11.2026. deploymentsafety.openai.com/gpt-6-cyber

18 BUILD: OPENAI KUPUJE SLOJ ZA PREGLED KODA

7. **OpenAI**. OpenAI to acquire Pierre Computer Company, Inc.. 04.11.2026. openai.com/index/openai-to-acquire-pierre/

19 BUILD: CONDUCTOR PRELAZI U METU

8. **Conductor**. Conductor is joining Meta. 04.11.2026. conductor.build/announcement

21 BUILD: COPILOT U XCODEU, BYOK I VEŠTINE AGENATA

9. **GitHub**. GitHub Copilot is now available in Xcode's coding assistant. 04.11.2026. github.blog/changelog/2026-11-04-github-copilot-is-now-availabl…
10. **GitHub**. BYOK and enterprise custom models in the Copilot usage API. 03.11.2026. github.blog/changelog/2026-11-03-byok-and-enterprise-custom-mod…
11. **GitHub**. Dependabot version updates support Agent Package Manager. 03.11.2026. github.blog/changelog/2026-11-03-dependabot-version-updates-sup…

22 BUILD: KO DOBIJA PORUKU KADA PROCURI KLJUČ

12. **GitHub**. Secret scanning upgrades detectors, adds SpaceX as partner. 05.11.2026. github.blog/changelog/2026-11-05-secret-scanning-upgrades-detec…
13. **GitHub**. CodeQL 2.27.4 improves accuracy and query metadata. 04.11.2026. github.blog/changelog/2026-11-04-codeql-2-27-4-improves-accurac…

23 BUILD: SVAKI PUSH PROLAZI KROZ AI PREGLED

14. **Vercel**. Introducing Vercel Security Review. 02.11.2026. vercel.com/blog/vercel-security-review
15. **Vercel**. Vercel Security Review now in public beta. 03.11.2026. vercel.com/changelog/vercel-security-review-public-beta

24 BUILD: BETTER AUTH: 12 UPOZORENJA ODJEDNOM

16. **Better Auth**. Security release on Tuesday, November 3, 2026. 03.11.2026. better-auth.com/blog/security-release-2026-11-03
17. **Vercel**. Better Auth November 2026 security release. novembar 2026. vercel.com/kb/bulletin/better-auth-november-2026-security-relea…

25 BUILD: SITNE PROMENE NA VERCELU

18. **Vercel**. Changelog. novembar 2026. vercel.com/changelog
19. **Vercel**. Projects can now be configured with vercel.toml. 02.11.2026. vercel.com/changelog/projects-can-now-be-configured-with-vercel…

26 MODEL WATCH: IMAGES 2.6: SLIKE DOBIJAJU POKRET

20. **OpenAI**. Introducing Images 2.6. 04.11.2026. openai.com/index/introducing-images-2-6/

27 MODEL WATCH: FLARE ILI SUNBURST

21. **OpenAI**. API pricing. novembar 2026. developers.openai.com/api/docs/pricing

28 MODEL WATCH: GOOGLE MEET RUŠI JEZIČKE BARIJERE

22. **Google Meet Help**. Use Speech Translation. novembar 2026. support.google.com/meet/answer/16221730
23. **Google Workspace Updates**. Real-time speech translation in Google Meet expands to 63 languages. 22.10.2026. workspaceupdates.googleblog.com/2026/10/real-time-speech-transl…

IZVORI / NASTAVAK

30 MODEL WATCH: MUSE DOBIJA GLAS I LICE

24. **Meta**. Give Your Muse a Voice. 05.11.2026. about.fb.com/news/2026/11/introducing-muse-ai-voice-expressive-…

32 MODEL WATCH: OD SKICE DO APLIKACIJE, OD TESTA DO ŽIVOTA

25. **OpenAI**. LifeVal. 02.11.2026. openai.com/index/lifeval/
26. **Google**. Turn sketches into apps with Gemini. 05.11.2026. blog.google/innovation-and-ai/products/gemini-app/turn-drawings…

33 SECURITY SIGNAL: GHOSTMAP: APLIKACIJA BEZ KODA KOJA RUŠI TELEFON

27. **Bitdefender Labs**. GhostMap: The Android flaw that crashes your phone before you open the app. 05.11.2026. bitdefender.com/en-us/blog/labs/ghostmap-android

35 PATCH NOW: ZAKRPITI ODMAH

28. **Canadian Centre for Cyber Security**. WordPress security advisory (AV26-1117). 03.11.2026. cyber.gc.ca/en/alerts-advisories/wordpress-security-advisory-av…
29. **WordPress.org**. WordPress 7.1.4 release. 28.10.2026. wordpress.org/news/category/releases/
30. **Zyxel**. Security advisory for out-of-bounds write vulnerability in GS1900 series switches. 03.11.2026. zyxel.com/global/en/support/security-advisories/zyxel-security-…
31. **Binarly**. Out-of-bounds write vulnerability in Zyxel GS1900 switches. novembar 2026. binarly.io/advisories/brly-2026-057

36 SECURITY SIGNAL: KADA SAJBERNAPAD PROMENI TEMPERATURU U FRIŽIDERU

32. **BleepingComputer**. Cyberattack disrupts blood storage refrigeration systems in France. novembar 2026. bleepingcomputer.com/news/security/cyberattack-disrupts-blood-s…
33. **CBS News**. Blood banks hit by cyberattack in France days after European freezer hacks. novembar 2026. cbsnews.com/news/cyberattack-france-blood-bank/
34. **NBC News**. Cyberattack on French blood bank fridges was thwarted. novembar 2026. nbcnews.com/world/france/france-cyberattack-blood-bank-refriger…

38 SECURITY SIGNAL: ZYXEL: TRI IZVORA, TRI RAZLIČITE STVARI

35. **Help Net Security**. Patched Zyxel GS1900 switches remained open to in-the-wild exploit. 05.11.2026. helpnetsecurity.com/2026/11/05/zyxel-cve-2026-107441-exploit/
36. **BleepingComputer**. Zyxel fixes zero-day exploited to hack nearly 1,000 network switches. novembar 2026. bleepingcomputer.com/news/security/zyxel-fixes-zero-day-exploit…

39 SECURITY SIGNAL: KADA JE POUZDAN IZVOR PROBLEM

37. **The Register**. Password manager mSecure tells users to change passwords, won't say why. 03.11.2026. theregister.com/security/2026/11/03/password-manager-msecure-te…
38. **BleepingComputer**. mSecure password manager hack prompts password reset warnings. novembar 2026. bleepingcomputer.com/news/security/msecure-password-manager-hac…
39. **Kotaku**. Hugely Popular RPG NIKKE Was Compromised. novembar 2026. kotaku.com/nikke-pc-client-compromise-malware-level-infinite-sh…
40. **Automaton**. Goddess of Victory: NIKKE PC launcher reportedly compromised in supply-chain attack. novembar 2026. automaton-media.com/en/news/goddess-of-victory-nikke-pc-launche…

40 SECURITY SIGNAL: PLAĆATI LJUDE DA NAĐU ONO ŠTO MODELI PROPUSTE

41. **OpenAI**. Rewarding defenders with bigger bug bounties. 02.11.2026. openai.com/index/rewarding-defenders-with-bigger-bug-bounties/
42. **DreamHost**. October Security Incident. 29.10.2026. dreamhost.com/news/announcements/october-security-incident/

41 SECURITY SIGNAL: KRATKI BEZBEDNOSNI PREGLED

43. **BleepingComputer**. Google Calendar phishing campaign hijacks sessions, bypasses MFA. novembar 2026. bleepingcomputer.com/news/security/google-calendar-phishing-cam…
44. **GitHub**. GitHub Desktop adds short-lived authentication tokens. 02.11.2026. github.blog/changelog/2026-11-02-github-desktop-adds-short-live…

44 LAB: CLAUDE I MISTERIJA ŠUPLJIH ČESTICA

45. **Anthropic**. Investigating vault particles with Claude. 04.11.2026. anthropic.com/research/investigating-vault-particles-with-claude

45 LAB: ZA ŠTA NAUČNICI ZAISTA KORISTE CLAUDE

46. **Anthropic**. How researchers use Claude. 05.11.2026. anthropic.com/research/how-researchers-use-claude

47 LAB: SAT VREMENA HEMIJE, NE SAT DO LEKA

47. **Google DeepMind**. Agentic cheminformatics with Google Antigravity. 03.11.2026. deepmind.google/blog/agentic-cheminformatics-with-google-antigr…

IZVORI / NASTAVAK

48 LAB: OD CAD MODELA DO STVARNOG DELA

48. **OpenAI**. Accelerating engineering for the physical world. 03.11.2026. openai.com/index/accelerating-engineering-for-the-physical-worl…

49 MONEY: AMD: DATA CENTER SKORO DUPLO VEĆI

49. **AMD**. AMD Reports Third Quarter 2026 Financial Results. 03.11.2026. newsroom.amd.com/news/amd-reports-third-quarter-2026-earnings/

51 MONEY: APPLE: REKORD BEZ AI PRIČE U BROJKAMA

50. **Apple**. Apple reports fourth quarter results. 02.11.2026. apple.com/newsroom/2026/11/apple-reports-fourth-quarter-results/
51. **Apple**. Apple unveils groundbreaking MacBook Pro with PROLED XDR display. 28.10.2026. apple.com/newsroom/2026/10/apple-unveils-groundbreaking-macbook…

52 MONEY: ARM PRODAJE NACRTE, A SADA I VIŠE OD TOGA

52. **The Motley Fool**. Arm Holdings Q2 2027 earnings call transcript. 05.11.2026. fool.com/earnings/call-transcripts/2026/11/05/arm-holdings-arm-…
53. **BigGo Finance**. Arm Holdings Q2 2027 earnings call summary. 04.11.2026. finance.biggo.com/news/US_ARM_2026-11-04

53 INFRA: KAKO IZGLEDA GARANCIJA OD 401 MEGAVAT

54. **Reuters preko KFGO**. TeraWulf gets credit backstop from Google for Anthropic data-center project. 04.11.2026. kfgo.com/2026/11/04/terawulf-gets-credit-backstop-from-google-f…
55. **CoinDesk**. Google could take ownership stake in TeraWulf's AI project if Anthropic defaults. 05.11.2026. coindesk.com/tech/2026/11/05/google-could-take-ownership-stake-…

54 INFRA: RAČUNARSKI KAMPUS KAO REZERVA ZA MREŽU

56. **OpenAI**. Grid Protectors Program. 02.11.2026. openai.com/index/grid-protectors-program/

55 MONEY: KO ZARAĐUJE U OVOJ FAZI

57. **Figma**. Figma Announces Third Quarter 2026 Financial Results. 04.11.2026. investor.figma.com/news-events/news/news-details/2026/Figma-Ann…

56 WORK: KAKO UKLJUČITI PREVOĐENJE U GOOGLE MEETU

58. **Meta**. WhatsApp Events brings people together beyond the group chat. 05.11.2026. about.fb.com/news/2026/11/whatsapp-events-brings-people-togethe…
59. **Android Authority**. Google Fitbit Edge launches with 7-day battery for $180. oktobar 2026. androidauthority.com/google-fitbit-edge-price-specs-features-la…
60. **Google**. Responsible AI for schools with Guided Learning. 03.11.2026. blog.google/products-and-platforms/products/education/ai-learni…

57 ORBIT: KRAJ MISIJE SWIFT

61. **NASA**. NASA's Swift Observatory Re-Entered Atmosphere. 04.11.2026. science.nasa.gov/blogs/swift/2026/11/02/nasas-swift-observatory…
62. **NASA**. NASA's Swift Mission Ends Ahead of Re-Entry. 23.10.2026. science.nasa.gov/blogs/swift/2026/10/23/nasas-swift-mission-end…

59 ORBIT: X-70 FRACTAL: AVION KOJI MENJA OPREMU

63. **NASA**. NASA Announces X-70 Experimental Aircraft to Advance Flight Research. 04.11.2026. nasa.gov/news-release/nasa-announces-x-70-experimental-aircraft…

60 ORBIT: DVA PRELETA, JEDNA FOTOGRAFIJA, JEDNO SLETANJE

64. **NASA**. NASA's Twin ESCAPADE Spacecraft to Slingshot Past Earth on Way to Mars. 02.11.2026. science.nasa.gov/blogs/escapade/2026/11/02/nasas-twin-escapade-…
65. **Space.com**. Dimorphos in sight: Europe's Hera probe gets its 1st look at battered space rock. novembar 2026. space.com/space-exploration/asteroid-comet-missions/dimorphos-i…
66. **NASA**. Safe and Precise Landing, Integrated Capabilities Evolution. 2026. nasa.gov/safe-and-precise-landing-integrated-capabilities-evolu…

61 USE THIS: PROVERITE SVOJE WORKFLOWE PRE 9. NOVEMBRA

67. **GitHub**. pull_request_target blocked by default December 2. 02.11.2026. github.blog/changelog/2026-11-02-pull_request_target-blocked-by…
68. **GitHub Docs**. Governing execution of GitHub Actions workflows. 2026. docs.github.com/en/repositories/managing-your-repositorys-setti…

62 USE THIS: NE UKIDAJTE ZAŠTITU ZBOG JEDNOG WORKFLOWA

69. **GitHub Docs**. Securely using pull_request_target. 2026. docs.github.com/en/actions/reference/security/securely-using-pu…

67 NEXT: ŠTA PRATIMO

70. **NASA**. NASA's Voyager 1 conserves power, resolves brief communications pause. 29.10.2026. science.nasa.gov/blogs/voyager/2026/10/29/nasas-voyager-1-conse…

o0o0o0o

/ 006

Šesti broj. Nedeljni pregled tehnologije,
besplatno, na tutorijali.app.

Izdanje 006
Datum 06.11.2026.
Period 31.10.2026. 00:00 → 05.11.2026. 22:15
Web tutorijali.app

tutorijali.app