



Vreme: 17.07.2026 14:00

Medij: telegraf.rs

Link: <https://www.telegraf.rs/hi-tech/info-tech/4361810-ai-napravio-chrome-dodatak-koji-za-nekoliko->

Autori: Nikola Momčilović

Teme: Evropska komisija

Naslov: AI napravio Chrome dodatak koji za nekoliko minuta zaobilazi EU proveru godina

2858

Istraživač je uz pomoć AI napravio Chrome dodatak koji za nekoliko minuta zaobilazi evropski sistem za proveru godina

Nova evropska aplikacija za proveru starosti korisnika suočila se sa ozbiljnim bezbednosnim problemom nakon što je istraživač pokazao da se njen sistem može zaobići jednostavnim Chrome dodatkom napravljenim uz pomoć veštačke inteligencije. Istraživač je demonstrirao da je njegov AI asistent napravio funkcionalnu zaobilaznicu za svega nekoliko minuta. Prema njegovim tvrdnjama, problem nije u pojedinačnoj grešci, već u samoj arhitekturi sistema koji se oslanja na poverenje u aplikaciju korisnika. Evropska komisija je ovu aplikaciju razvila kao deo šire inicijative za zaštitu dece na internetu, ali njena sposobnost da pouzdano potvrdi godine korisnika sada je dovedena u pitanje. Evropska aplikacija predstavljena je u aprilu, a već tada je bezbednosni istraživač uspeo da je zaobiđe za manje od dva minuta. Nakon toga usledilo je nekoliko ažuriranja, uključujući poslednju verziju objavljenu 10. jula. Ipak, ni nakon više od 2.400 izmena koda na GitHubu, aplikacija i dalje ima problem sa osnovnom funkcijom zbog koje je napravljena, odnosno pouzdanom proverom starosti korisnika. Istraživač je ponovo pokazao da je moguće napraviti Chrome ekstenziju koja aplikaciji šalje lažne podatke o potvrdi godina. Tokom demonstracije sistem je prihvatio podatke koje je dostavio dodatak, bez skeniranja pasoša, prepoznavanja lica ili povezivanja sa konkretnim uređajem. Prema tvrdnjama istraživača, ovakav propust nije moguće jednostavno popraviti malom zakrpom. Potrebna bi bila promena celokupne arhitekture sistema kako bi se uklonilo oslanjanje na anonimne sesije i proverilo da li je aplikacija korisnika izmenjena. Trenutni model funkcionise tako što veruje da klijentska aplikacija nije promenjena. Međutim, takav pristup može biti problematičan bez dodatne hardverske autentifikacije ili sistema poput zaštite integriteta aplikacija na platformama kao što je Google Play. Evropska komisija je razvoj aplikacije poverila nemačko-švedskom konzorcijumu, koji je u januaru 2025. godine dobio ugovor vredan 2 miliona evra na period od 24 meseca. Plan je bio da aplikacija funkcionise kao digitalni novčanik za čuvanje dokaza o starosti korisnika u obliku digitalnog sertifikata. Ovaj slučaj pokazuje koliko veštačka inteligencija može ubrzati pronalaženje slabosti u softveru. Istraživač tvrdi da mu je AI alat omogućio da razvije čitav koncept zaobilaženja sistema za samo nekoliko minuta. Ipak, stručnjaci upozoravaju da ovakvi sistemi moraju biti projektovani tako da ne zavise samo od poverenja u uređaj i aplikaciju koju korisnik kontroliše. Kako evropske zemlje sve više uvode obavezne provere godina za pristup određenim internet sadržajima, sigurnost ovakvih rešenja biće jedan od ključnih izazova u narednim godinama. (Telegraf.rs)

