Používate lacné smart okuliare? Dajú ovládnuť cez Bluetooth a útočník sa dostane k fotkám

Datum	23.9.2026
Subjekt	Zajtra studio spol. s r.o.
Autor	Lenka Ivančíková
Region	Slowakei
Kategorie	IT und Kommunikation

Výskumníci zo spoločností NSB Cyber a Abstract Shield otestovali dva lacné páry smart okuliarov a našli v nich vyše desať chýb. Netýkali sa len samotných okuliarov, ale aj ich aplikácie a pridruženej webovej stránky. Informuje o tom portál Malwarebytes Labs, ktorý sa odvoláva na testy austrálskej ABC.

Testované kusy stáli **60 a 110 austrálskych dolárov**, teda približne 42 a 78 amerických dolárov. Hlavným problémom je nezabezpečené párovanie cez Bluetooth. Ak boli okuliare zapnuté a nepripojené k telefónu majiteľa, útočník sa k nim vedel pripojiť ako prvý, **bez hesla a bez akéhokoľvek potvrdenia**.

Po pripojení sa dá fotiť aj kopírovať obsah

Keď sa útočník raz pripojil, mohol okuliare ovládať. Podľa testov vedel **vyhotoviť fotografie alebo nahrávky**, skopírovať už uložený obsah a zachytávať údaje prenášané medzi okuliarmi a telefónom. Dokázal tiež vydať iné zariadenie za okuliare obete a pripojiť ho k jej mobilnej aplikácii. Identifikátor viditeľný cez Bluetooth sa navyše dal spojiť so slabinou na webe aplikácie a získať tak **e-mailovú adresu a dátum narodenia** používateľa.

Rayban Meta Glasses

Druhý problém sa týka ochrany súkromia. Hlas alebo text zadaný do vstavanej umelej inteligencie a odoslané obrázky putovali najprv na **server v čínskom Šen-čene** a odtiaľ mohli pokračovať ďalej. Testy nezistili, ako sa s údajmi následne nakladalo. Z umiestnenia serverov a z odpovedí chatbota výskumníci usúdili, že asistent aspoň sčasti stojí na čínskych štátnych modeloch umelej inteligencie.

Nemali by ste prehliadnuť:

- **Samsung ukázal smart okuliare s AI. Ponúknu živé preklady aj navigáciu**
- **Povinná aktualizácia pre Meta Ray-Ban okuliare: Bez viditeľnej LED diódy nebudú nahrávať**
- **Nepoužívate pri počítači okuliare s blokovaním modrého svetla? Toto by ste mali vedieť**

Normy platia, no až od marca a len v Austrálii

Austrálske bezpečnostné normy pre inteligentné zariadenia sa vzťahujú na väčšinu spotrebiteľských produktov vyrobených **4. marca 2026** a neskôr. Vyžadujú okrem iného žiadne univerzálne predvolené heslá, spôsob hlásenia zraniteľností a informáciu o minimálnej dĺžke podpory aktualizácií. Zariadenia vyrobené skôr pod ne nespadajú. Profesorka Kimberlee Weatherall k tomu poznamenala, že pravidlá vyžadujú jedinečné heslo, no zdá sa, že výrobca heslo nepoužíval vôbec.

Xiaomi Mijia Smart Audio Glasses - majú fyzické párovanie stlačením nožičky | Zdroj: Lenka Ivančíková

Pre slovenského kupujúceho z toho plynie nepríjemný záver. Okuliare tohto typu sa k nám bežne dostávajú z čínskych obchodov. Austrálske normy tu neplatia. Malwarebytes preto radí vyhnúť sa lacným okuliarom s kamerou, ktoré nemajú **jasný fyzický krok párovania**, teda napríklad stlačiť nejakyý prvok na konštrukcii okuliarov, overenie účtu, zverejnený kontakt na hlásenie chýb a uvedené obdobie podpory. Ak už také rizikové zariadenie máte, oplatí sa prestať používať jeho cloudové funkcie pri citlivom obsahu a odobrať aplikácii zbytočné oprávnenia.

Konkurencia medzitým pripravuje svoje

Samsung sa nechal odhaliť ešte pred predstavením tabletov Galaxy Tab, takže o novinke sa vie prakticky všetko dopredu. Google zas priznal incident, pri ktorom Gemini prenikol do systémov firiem počas bezpečnostného testu, čo je ďalšia ukážka toho, ako rýchlo sa mení hranica medzi nástrojom a hrozbou. A Xiaomi zverejnilo harmonogram aktualizácií HyperOS 4 pre európske telefóny.

https://www.mojandroid.sk/lacne-smart-okuliare-sa-daju-ovladnut-cez-bluetooth-utocnik-sa-dostane-k-fotkam