# Stačí jeden videohovor a hacker sa môže dostať do telefónu. Ohrozené sú lacnejšie zariadenia

**18.8.2026 - Tomáš Kanálik | Zajtra studio spol**

**Výskumníci zo skupiny SSD Secure Disclosure opísali dvojstupňový postup, ktorý sa cez prijatý videohovor dostane až k jadru Androidu. Portál The Hacker News upozorňuje, že ide o telefóny s modemom Unisoc, teda o najlacnejšiu triedu, a výrobca čipu na hlásenie zatiaľ nereagoval.**

Zverejnenie vyšlo **17. augusta** a je druhým stupňom reťazca, ktorý sa začal už v marci. Vtedy tá istá skupina ukázala, že sa cez poškodený videohovor dá spustiť cudzí kód priamo vo firmvéri modemu. Nový diel na to nadväzuje a z modemu sa dostane do pamäte, v ktorej beží samotný systém. Bez prvého kroku druhý nefunguje, dokopy však tvoria **úplnú cestu k jadru**.

## Ktorých telefónov sa to týka

Chyba sedí vo firmvéri modemu, ktorý zdieľa najmenej trojica čipov: **T606** v Motorole E13, **T612** v Realme C33 a **T7250** v modeli Redmi A5. Sú to telefóny z najlacnejšej police, ktoré sa u nás bežne predávajú. Unisoc, kedysi známy ako Spreadtrum, dodáva čipy pre zariadenia vo vyše **140 krajinách** a okrem Motoroly a Realme ich odoberá aj Xiaomi.

Motorola Moto e13 | Zdroj: Motorola

Zoznam zasiahnutých čipov je zatiaľ krátky a všetky tri menované modely patria do najlacnejšej triedy. Zvýšenie oprávnení výskumníci potvrdili na Motorole E13 so záplatou z **februára 2025** a na Redmi A5 so záplatou z **januára 2026**. Boli to teda telefóny, ktoré mali zabezpečenie v poriadku, a útok aj tak prešiel.

## Prečo sa to vôbec dá

Podstata je v tom, že modem a hlavný procesor v čipe Unisoc zdieľajú **tú istú fyzickú pamäť** a nedelí ich žiadna hardvérová hranica. Keď útočník ovládne modem a sprístupní si čítanie, zápis aj spúšťanie. Sú v ňom aj stránky, na ktorých beží jadro.

Dobrá správa je, že spustiť to z ulice nikto nedokáže. Útočník musí ovládať vlastnú sieť s VoLTE, mať za sebou marcovú chybu a obeť musí videohovor prijať. Ide teda o **cielený zásah**, nie o plošný malvér, aký chodí cez aplikácie a stačí mu neopatrné klepnutie.

Zaplátať sa to zatiaľ nedá. Augustový bezpečnostný bulletin Androidu vyšiel skôr a túto chybu nerieši, vlastný bulletin Unisocu k nej neexistuje. Výskumníci píšu, že výrobcu skúšali osloviť e-mailom aj cez LinkedIn a **nedostali odpoveď**. Rovnakú vetu obsahovalo aj marcové zverejnenie, takže mlčanie trvá už niekoľko mesiacov.

**Nemali by ste prehliadnuť:**

- **Motorola spúšťa beta program Androidu 17 pre ďalšie smartfóny. Je medzi nimi aj váš?**

- **Motorola začala s distribúciou stabilného Androidu 16 pre prvé dva modely**
- **Samsung končí s podporou série Galaxy S23. Kedy príde posledná veľká aktualizácia?**

Majiteľom takého telefónu zostáva jediné: sledovať, či výrobca vydá aktualizáciu firmvéru. Istotu však nikto nedáva. Kaspersky opísal ten istý architektonický nedostatok už v novembri **2025** na inom čipe Unisocu a jednu z ciest označil za hardvérovú, teda softvérom neriešiteľnú. Tá dnešná sa opraviť dá, Unisoc sa k tomu ale nezaviazal. Podobnú chybu z roku **2022** pritom vtedy opravil a náprava sa rozposlala cez bulletin Androidu.

https://www.mojandroid.sk/unisoc-videohovor-hrozba