Spordikäevõrud - uus andmelekke turvarisk

11 aastat tagasi - 13.04.2015 Autor: AM

Infot lekib Internetti ühendatud seadmete ajastul igalt poolt. Nüüd selgub, et ka meie nutikad käevõrud võivad üht-teist lekitada, avastas Kaspersky Lab, tuntud antiviirusetootja.

Tuleb välja, et viimasel ajal laialt levinud fitnessijälgimisseadmed, mis koguvad andmeid kasutaja aktiivsuse kohta, võivad neid andmeid edastada ka teistele kui ainult otsesele omanikule. See spordikäevõrude omadus avastati, kui Kaspersky Lab uuris, kuidas käevõrud vahetavad andmeid nutitelefonidega.

Selgus, et ühendatava seadme autentimise meetod, mida mitmes populaarses fitness-käevõrus kasutatakse, annab kõrvalistele inimestele võimaluse märkamatult nutitelefoniga ühenduda, selles käske täita ja isegi vidinasse salvestatud andmeid alla laadida. See kõik on võimalik siis, kui nutitelefon töötab Androidi operatsioonisüsteemi versiooniga 4.3 või uuemaga ja kui selles on autoriseerimata rakendus spordikäevõruga sünkroonimiseks.

Teatavasti peab kasutaja fitnessijälgimisseadme ja nutitelefoni vahel ühenduse loomiseks selle tegevuse kinnitama, vajutades käevõrul vastavat nuppu. Kuna enamikul praegu kasutatavatest käevõrudest ei ole ekraani, saavad kurikaelad sellest tingimusest kergesti mööda hiilida: kui fitness-käevõru nutitelefoniga ühendumise kinnituse küsimiseks vibreerib, ei või kasutaja kuidagi teada, kas

tegemist on tema enda või kellegi teise telefoniga.

Spordikäevõrud, mida Kaspersky Lab uuris, edastasid nutitelefoniga sünkroonimisel andmeid ainult kasutaja tehtud sammude arvu kohta. Järgmise põlvkonna jälgimisseadmed koguvad aga inimese füüsilise seisundi kohta juba oluliselt rohkem andmeid, mis tähendab märgatavalt suuremat konfidentsiaalsete andmete lekke ohtu.

> *Kui fitness-käevõru nutitelefoniga ühendumise kinnituse küsimiseks vibreerib, ei või kasutaja kuidagi teada, kas tegemist on tema enda või kellegi teise telefoniga.*

„Muidugi pole avastatud ohud samaväärsed selliste kriitiliste andmete nagu salasõnade või pangakaardi andmete lekkimise ohuga. Meie tehtud katse räägib aga siiski sellest, et populaarsetel elektroonikavidinatel on turvaauke, mida kurikaelad saavad ära kasutada. Praeguse põlvkonna fitnessijälgimisseadmete funktsioonid on praegu veel piiratud: peamiselt loevad nad samme ja jälgivad unefaase, aga need vidinad arenevad. Just seepärast tuleks juba praegu mõelda nende turvalisuse tagamisele, et leida ohutu viis spordikäevõrude ja nutitelefonide sünkroonimiseks," ütleb Kaspersky Labi viirusetõrjeekspert Roman Unuchek.

Fitnessikäevõrude kasutajatel, kes soovivad veenduda oma vidina turvalisuses, soovitab Kaspersky Lab vidina arendusettevõtte poole pöörduda ja uurida, kas ülalkirjeldatud rünnak on selle firma jälgimisseadmete puhul võimalik.

Täpsemalt saab lugeda fitnessikäevõrude turvaaukude kohta Kaspersky Labi aruandest.

Foto: (CC) Skeeze / Pixabay

- Uudised

- Turvalisus
- Tarkvara