FragAttacki turvaaugud ohustavad miljoneid seadmeid ja puudutavad WiFi standardit ennastki

5 aastat tagasi - 13.05.2021 Autor: AM

Belgia küberturvalisuse ekspert Mathy Vanhoef avastas ligi 12 erinevat haavatavust, mis mõjutavad suurt hulka WiFi seadmeid. Vanhoef pani nende haavatavuste kogumile nime FragAttacks ja tegi sellekohase veebisaidi, kust saab turvaaukude kohta põhjalikumat tehnilist infot: vaata www.fragattacks.com. Ekspert väidab, et ründajad saavad neid nõrkusi kasutades ligi kasutaja andmetele.

Oht puudutab igasuguseid WiFiga seadmeid nutitelefonidest ja arvutitest ruuteriteni. Ründaja peab asuma seadme WiFi levialas.

FragAttacksi lehel kirjeldatakse, et turvanõrkus on põhjustatud nii programmeerimisvigadest tootja tarkvaras kui ka Wi-Fi Alliance´i standardis endas. Standardit puudutavad kolm turvaohtu kaheteistkümnest avastatust.

Kõigi WiFi kasutajate lohutuseks mainib Vanhoef, et FragAttacksi ärakasutamine on üsna keeruline ja nõuab sügavamaid teadmisi. Aga eks on vaid aja küsimus, kui selle kõige lihtsustamiseks luuakse vastavad sissemurdmise tööriistad.

Siin videos kirjeldatakse FragAttacksi olemust lähemalt:

Selle ennetamiseks on paljud tootjad juba välja tulnud oma tarkvarauuendustega, mis esialgu FragAttacksi augud ära lapib. Microsoft näiteks tõi välja kolm turvauuendust Windowsile (siin, siin ja siin), mis selle ohu likvideerivad - seega Windowsi värskenduste paigaldamine juba aitab.

Netgeari FragAttacksi turvaohu jaoks loodud lehel öeldakse, et ründajal on lisaks WiFi levialas olemisele vaja teada ka selle parooli. Samal lehel on ka seadmete loetelu, mis on turvauuenduse saanud.

Soovitused, kuidas FragAttacksi rünnakuid ära hoida, on lihtsad:

- ära jaga oma WiFi võrgu parooli kõrvalistele isikutele
- kasuta tugevat, raskesti äraarvatavat parooli ja muuda seda piisavalt tihti
- Jälgi oma WiFi võrku, et sinna poleks ühendatud tundmatud seadmed (kasuta näiteks oma ruuteri äppi või seadistuste lehekülge selle jaoks)
- kasuta veebilehtedele sisselogimiseks või tundliku info edastamiseks vaid neid saite, mis kasutavad HTTPS-i (sel juhul rünnaku alla sattunud võrgus sinu andmed ei leki)

The Verge kirjutab, et nüüdseks on juba pikka aega eksisteerinud turvanõrkuste vastu oma uuendustega välja tulnud terve rida tootjaid: Aruba, Cisco, Ruckus, Intel, Juniper, Lancom, Lenovo, Linux Wireless, Samsung, Synology, Zyxel jt.

- Uudised

- Andmeside
- Tarkvara
- Turvalisus
- Võrguseadmed

Pilt