Cloudbleed - pilveleke, mis võib jälle paroolid ula peale jätta

9 aastat tagasi - 25.02.2017 Autor: AM

Kõik teenused kolivad vaikselt pilve ja isegi soovitatakse sinna minna - siis on kõik andmed kuskil turvalises serveris hoiul ja kui oma asjadega midagi juhtub, saab pilvest kõik kätte. Ohtlik on aga see, et pilv võib lekkida. Cloudbleed on ohtlik pilveleke, mis jättis eelmise aasta 22. septembrist alates paljude tuntud teenuste andmed, sealhulgas paroolid võõrastele kättesaadavaks. Õnneks puudutas see vaid vähest osa Cloudflare´ist, kuid ikkagi - tähtsad andmed on lekkinud ja kuhu ning kui palju Internetiavarustes, seda ei tea keegi.

Täpsemalt tähendab Cloudbleed vea tõttu mäluleket. Lähemalt saab lugeda siit.

Kes võivad olla sellest mõjutatud, selgub Cloudflare´i kasutatavate veebide nimekirjast. Siit lehelt saab sisestada teenuse ja teada saada, kas teenus on Cloudflare´i pilveteenuse kasutaja või mitte. Nimekiri on pikk, mõjutatud võivad olla üle 4,2 miljoni veebisaidi. Kuulsaimad teenused, mis Cloudflare´i kasutavad, on näiteks FitBit, Yelp, Medium, CodePen, OKCupid, Uber, Transferwise.

Ka paarsada IOS-i äppi on lekkest mõjutatud, nende nimekirja leiab siit.

Mida siis nüüd teha? Loomulikult sedasama, mida viimaste aastate suurte lekete puhul ikka - muuta ära oma paroolid kõigil mõjutatud lehekülgedel ja nendes teenustes, kus oli kasutusel sama parool.

Seda, kas ja kust on veel andmeid võib-olla lekkima läinud, saab vaadata sellelt lehelt. Sisesta oma e-posti aadress ja lekkekohad antakse teada.

- Uudised

- Tarkvara
- Turvalisus

Pilt

