Sigurnosno osjetljivi WPA2

 U nedavno objavljenom radu grupa autora tvrdi da WPA2 zaštita ima sigurnosne propuste koji otvaraju prostor napadu kojim je moguće grubom silom dočepati se pristupa mreži. Slično napadima na WPA protokol, napad grubom silom na proces deautentikacije otvara vrata ne tako sofisticiranoj tehnici kojom se metodom pokušaja i pogreške pogađa lozinka.

Tako je, eto, nakon WEP-a pao i WPA2, barem po tvrdnjama autora članka zaklonjenog iza paywalla ("plati pa čitaj"). No to ne znači da trebamo u panici gasiti bežične mreže. Riječ je o napadu metodom pokušaja i pogreške, te kako i sami autori u svom radu navode, dovoljno dugačka i dovoljno komplicirana lozinka i dalje će biti ozbiljna prepreka napadačima, tim više što je napada na WPA2-PSK bilo i ranije, a i za njih vrijedi isto pravilo.

No informatička povijest nas uči da oslanjanje samo na kompleksne lozinke nije dovoljna zaštita. Zbog toga valja biti na oprezu: iako je uz dovoljno kompleksnu lozinku ovaj sigurnosni propust relativno minorna opasnost, budućnost bi mogla (zapravo, usudio bih se reći: "sigurno će") pokazati kako ta zaštita više nije baš tako dobra.

U međuvremenu trebate osigurati samo dvije stvari:

- koristite dugačku, kompliciranu lozinku (WPA2 prihvaća do 63 znaka za lozinku, odnosno do 64 heksadecimalna znaka) koja ne sadrži riječi i izraze koje je lako pogoditi korištenjem rječnika;

- pobrinite se da vaši WiFi uređaji imaju isključen WPS jer ga je zaista lako razbiti, a jednom razbijen WPS rado će napadaču isporučiti pristupnu lozinku.

sri, 2014-04-02 06:38 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [1]
Kategorije: Mrežna sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1378

Links
[1] https://sysportal.carnet.hr/taxonomy/term/14
[2] https://sysportal.carnet.hr/taxonomy/term/33