Misfortune Cookie

 Prije nekoliko dana grupa istraživača iz tvrtke Check Point Software Technologies [1] pronašli su propust u web sučeljima kućnih routera nekoliko velikih proizvođača takvih uređaja. Procjenjuje se da bi broj ranjivih uređaja mogao biti preko 12 milijuna. Proizvođači čiji uređaji mogu biti ranjivi su (i kod nas popularni) D-Link, ZTE, Zyxel, TP-Link i drugi. Puni popis možete naći u datoteci na adresi http://mis.fortunecook.ie/misfortune-cookie-suspected-vulnerable.pdf [2].

Ranjivost ovako velikog broja uređaja je moguća zbog toga što svi oni rabe *embedded* web-poslužitelj RomPager. Napad se izvodi pomoću posebno oblikovanog HTTP kolačića, pomoću kojeg se odmah mogu dobiti administrativna prava na uređaju. Što je od tamo moguće, jasno je svima: DoS, snifanje prometa, daljnji prodor u vašu kućnu mrežu ili mrežu tvrtke.

Na adresi https://rompager.hboeck.de [3] postoji alat s kojim možete provjeriti jeste li ranjivi, no nemamo informaciju o njegovoj pouzdanosti. U svakom slučaju, za obranu možete ugasiti HTTP i prijeći na HTTPS, ugasiti pristup web-sučelju preko interneta, te nadograditi firmware samog routera (ukoliko je izašao onaj koji je pokrpao ovu rupu).

Ono što je zanimljivo (ajmo to tako reći) je da se za ranjivost zna od 2002. godine, i rupa je pokrpana 2005. godine. Nju je napravio AllegroSoft, proizvođač RomPagera. No, neki routeri proizvedeni 2014. godine su još uvijek rabili zastarjeli softver, pa je očigledno da *industrija* slabo mari za krajnje korisnike i pouzda se u *security through obscurity* model, tipičan za zatvoreni softver.

Zasad nema prijavljenih provala putem ove ranjivosti, pa su neki komentatori rekli da se radi jednostavno o marketinškoj akciji tvrtke Check Point.

No, ostaje nam za misliti koliko je siguran firmware na uređajima koje rabimo i na koji nemamo nikakvog utjecaja? U ovom slučaju, možemo si pomoći tako da odabremo model koji podržava neki od slobodnih firmwareova tipa OpenWRT, ali uređaja koji imaju direktan pristup na internet je sve više (primjerice, pametni televizori).

Izgleda da će nam u budućnosti zanimacija biti zamjena tvorničkih firmwareova nekim otvorenim (i pretpostavljamo) sigurnijim softverima...

Više o svemu možete potražiti na adresi: http://mis.fortunecook.ie/ [4]

ned, 2014-12-28 01:39 - Željko Borš**Vijesti:** Sigurnosni propusti [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1484

Links
[1] http://www.checkpoint.com/
[2] http://mis.fortunecook.ie/misfortune-cookie-suspected-vulnerable.pdf
[3] https://rompager.hboeck.de
[4] http://mis.fortunecook.ie/
[5] https://sysportal.carnet.hr/taxonomy/term/14