Ranjivost FREAK u SSL-u

Već smo se nekako privikli na redovito pojavljivanje propusta u SSL-u. Ovaj put nije riječ toliko o propustu samog protokola, nego je više riječ o ljudskom faktoru. Točnije državnom, američkom. Inače, sigurnosni eksperti su, kao i drugim ranjivostima, i ovom nadjenuli zanimljivi naziv **FREAK (Factoring attack on RSA-EXPORT Keys)**. Logotip još nisu napravili, ali ne sumnjamo da hoće.

Vrlo vjerojatno znate, još prije samo petnaestak godina vrijedila je zabrana izvoza kriptografskog softvera izvan teritorija SAD-a. Bilo je dopušteno "izvoziti" samo softver sa slabim kriptografskim ključevima od 40 bita (takozvani **RSA-EXPORT cipher**), kako bi se mogao održavati kakav-takav sigurni promet. Danas je, zbog snažnijeg hardvera koji može brzo razbiti ovakvu enkripciju, zaštita ovako slabim ključevima smiješna, pa je navedena restrikcija ukinuta. No, programski kod **nije maknut** iz softvera, pa je pronašao svoj put na Android i iOS.

Zbog buga u implementaciji SSL-a na drugoj strani, onoj poslužiteljskoj, moguće je ostvariti komunikaciju s ovako slabom enkripcijom. Procjenjuje se da je takvih poslužitelja oko trećine od svih u produkciji. No, opasnost postoji, a na vama je da i dalje nadograđujete svoje poslužitelje, te ukinete sve starije algoritme, i to u svim servisima koji rabe SSL.

Kako ćete znati jeste li ranjivi? Android i iOS će biti zakrpan redovitim nadogradnjama, ako je vaš uređaj još podržan. U protivnom, možete rabiti mobilne inačice preglednika Chrome ili Firefox, koje nemaju ovaj problem (ugrađeni preglednici na obje platforme su ranjivi).

Situaciju na poslužiteljskoj strani možete provjeriti na ovaj način:

```
$ openssl s_client -connect www.carnet.hr:443 -cipher EXPORT
CONNECTED(00000003)
3074328728:e
rror:14077410:SSL routin
es:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure:s23_clnt.c:749:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 114 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
---
```

Ukoliko dobijete poruku "**handshake failure**", niste ranjivi na FREAK, jer vaš poslužitelj nije

spreman komunicirati na slabim "EXPORT" algoritmima.

Više informacija možete naći na ovim stranicama [1], ali i na mnogobrojnim drugim koje upravo nastaju.

sri, 2015-03-04 16:29 - Željko Boroš**Vijesti:** Sigurnosni propusti [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1526

Links
[1] http://www.zdnet.com/article/freak-another-day-another-serious-ssl-security-hole/
[2] https://sysportal.carnet.hr/taxonomy/term/14