DROWN with the SSL2!


Ako kojim čudom, previdom ili legendarnom administratorskom lijenošću vaši poslužitelji još uvijek omogućuju komunikaciju korištenjem SSL2 protokola, DROWN [1] napad trebao bi biti konačni argument za bacanje tog starog i provjereno ranjivog protokola u ropotarnicu kriptografske povijesti.

Punim nazivom "Decrypting RSA with Obsolete and Weakened eNcryption", ovaj vrlo ozbiljan napad omogućuje napadaču (pozicioniranjem kao MITM između klijenta i poslužitelja) vrlo brzo provaljivanje komunikacijskog kanala i posljedično potpuno prisluškivanje prometa.

Napad na SSL2 protokol moguć je zbog korištenja starog “export-grade” kriptografskog algoritma, pa provaljivanje ne troši previše resursa. Dapače, dio poslužitelja osjetljivih na taj napad koristi OpenSSL verziju koja sadrži bug čije postojanje značajno olakšava provalu: poslužitelje koji su osjetljivi na DROWN i pritom imaju i taj bug moguće je razbiti za nešto više od jedne minute korištenjem “običnog” kućnog ili uredskog računala.

Stvar se dodatno komplicira u ne tako rijetkom slučaju da ranjivi poslužitelj koji koristi SSL2 dijeli isti RSA ključ sa poslužiteljem koji koristi značajno sigurniji TLS protokol: u tom slučaju, jednom razbijen SSL2 poslužitelj omogućit će uspješno izvođenje napada na inače siguran TLS poslužitelj pomoću Bleichenbacherova [2] napada - napadač može u kratkom vremenu (svega nekoliko sati) i uz mali trošak (oko 440$ za Amazon EC2, tvrde autori) razbiti komunikacijski kanal.

Drugim riječima, imate li u svojoj mreži samo jedan poslužitelj osjetljiv na DROWN napad, te ako među poslužiteljima dijelite isti ključ, svi vaši poslužitelji bit će izloženi ozbiljnom sigurnosnom riziku!

Rješenje problema je, naravno, vrlo jednostavno: isključite podršku za SSL2 na vašim poslužiteljima.

Drugi dobar savjet je – ako to nije apsolutno nužno, nemojte dijeliti ključeve na više poslužitelja.

Nakon toga, naravno, instalirajte i nove verzije OpenSSL-a (ali to i tako redovito radite, zar ne?)

Iako se lakoća ove zakrpe čini trivijalna, autori tvrde da je oko trećine poslužitelja na Internetu ranjivo, što zbog korištenja SSL2 podrške, što zbog dijeljenja ključeva među poslužiteljima – razlog više da se SSL2 podrške riješimo jednom za svagda.

Detaljnije informacije o napadu i whitepaper možete pronaći na web stranici [3] The DROWN Attack, gdje se nalazi i alat kojim možete provjeriti jesu li vaši poslužitelji osjetljivi na ovaj napad.

pet, 2016-03-04 00:24 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1620

Links
[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=2016-0800%20
[2] https://www.ietf.org/mail-archive/web/openpgp/current/msg00999.html
[3] https://drownattack.com/#paper
[4] https://sysportal.carnet.hr/taxonomy/term/14