# Heartbleed bug, dio drugi

Taman smo se oporavili od potresa nazvanog Heartbleed [1], a već nam na vrata kuca nastavak iste priče. Kao i u slučaju originalnog propusta, riječ je o programerovoj pogrešci koja je ostala skrivena dugo vremena (točnije, cijelo jedno desetljeće i pol), a koja napadaču otvara prostor za prilično lako izvediv napad.

Iskorištavanjem propusta u handshake proceduri (preciznije: injektiranjem malicioznih paketa) osoba koja je u mogućnosti pozicionirati se kao MiTM (*Man in The Middle* – osoba preko čije infrastrukture prolazi promet između dvije točke) u prilici je prisiliti obje točke da za SSL enkripciju koriste predvidive ključeve koje je zatim moguće razbiti. Veza uspostavljena na takav način po svojim je karakteristikama posve legitimna SSL konekcija, ali je njena sigurnost ozbiljno kompromitirana zato što se ne koriste sigurni ključevi, već oni koje napadač može razbiti i u relativno kratkom vremenu biti u mogućnosti prisluškivati komunikaciju SSL kanalom.

Ovaj problem nešto je manje neugodan od originalnog Heartbleed problema, jer se napadač mora nalaziti na komunikacijskom putu između točke A i točke B, ali njegovu ozbiljnost ne trebamo zanemariti imajući na umu brojnost bežičnih veza i točaka s otvorenim pristupom Internetu (kafići, aerodromi i sl.) gdje je zapravo prilično jednostavno "ugurati se" u vezu između dvije točke.

Problem je vezan isključivo uz OpenSSL – koristite li neko drugo rješenje možete biti mirni. Koristite li pak OpenSSL, provjerite jeste li već instalirali sigurnosnu zakrpu za ovaj problem.

Detalje o propustu i Python skriptu za provjeravanje ranjivosti vaših servera možete pronaći na stranicama trvrtke Tripwire. [2]

sri, 2014-06-11 06:14 - Radoslav Dejanović**Vijesti:** Sigurnost [3]
**Vote:** 5

Vaša ocjena: Nema Average: 5 (1 vote)

**Source URL:** https://sysportal.carnet.hr./node/1406

**Links**
[1] https://sysportal.carnet.hr./node/1382
[2] http://www.tripwire.com/state-of-security/incident-detection/detection-script-for-cve-2014-0224-openssl-cipher-change-spec-injection
[3] https://sysportal.carnet.hr./taxonomy/term/13