Hartbleed živi dalje

 Dva mjeseca nakon otkrića opasnog Heartbleed sigurnosnog propusta u OpenSSL biblioteci, nešto više od polovice ranjivih servera je patchirano, dok je, kako tvrdi [1] Errata Security, ostatak i dalje osjetljiv na napad.

Iako testiranje nije obavljeno na rigorozan način (korištena je poprilično jednostavna metoda [2] - skeniran je samo port 443), pa brojka nije posve pozdana, imamo razloga vjerovati kako je unatoč tome broj ranjivih strojeva na Internetu pozamašan. Kako sam autor softvera za testiranje ranjivosti tvrdi, nakon inicijalne panike po objavi sigurnosnog propusta, kada se u kratkom roku prepolovio broj ranjivih servera, brzina patchiranja drastično je opala: razlog tome može biti jedan od dva slučaja: ostali su nepatchirani uređaji koje iz nekog razloga nije bilo moguće zakrpati (*embedded* uređaji, primjerice) i serveri koji nisu patchirani zbog lijenosti/neznanja administratora ili nerazumne poslovne odluke. U tu grupu svakako treba ubrojiti i potencijalne *embedded* uređaje za koje je u međuvremenu izdan novi firmware, ali koji iz sličnog razloga nisu osvježeni popravljenom verzijom.

U svakom slučaju, brojka od 309,197 sustava koji su još uvijek potencijalno ranjivi tjera na razmišljanje.

čet, 2014-06-26 08:58 - Radoslav Dejanović**Vijesti:** Sigurnost [3]
Kategorije: Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1410

Links
[1] http://blog.erratasec.com/2014/06/300k-vulnerable-to-heartbleed-two.html#.U6e_iR1UmHv
[2] http://blog.erratasec.com/2014/05/300k-servers-vulnerable-to-heartbleed.html#.U6Yi2vldWPB
[3] https://sysportal.carnet.hr/taxonomy/term/13
[4] https://sysportal.carnet.hr/taxonomy/term/28