Apple: još malo SSL ispravaka

Čini se kako frka oko programerskih propusta u međuoperacijskosustavnom okruženju još nije završila: Apple je ispravio [1] nekoliko ne baš bezazlenih propusta u svojoj implementaciji SSL protokola; propust je nazvan "**triple handshake bug**", a napada jednako mobilni iOS i "stolni" OS X, omogućujući napadaču da izvede MITM [2] napad i efektivno prisluškuje promet između korisnika i servera.

Iako tvrtka tvrdi kako je ovaj propust sa stanovišta sigurnosti daleko benigniji od "goto fail" i "Heartbleed" propusta, tu tvrdnju treba uzeti s vrećom soli: po svojim posljedicama po korisnika jednako je opasan.

Vlasnicima Macintosha i mobilnih iUređaja najtoplije se preporučuje preuzimanje sigurnosnih zakrpa (objavljene su zakrpe za OS X 10.6 i viši, te iOS 7.1). Također, Apple je posve neočekivano – jer, rekoše, njihov hardver nije ranjiv [3] - izdao "Heartbleed" zakrpe za Airport Extreme i Time capsule.

pet, 2014-04-25 07:30 - Radoslav Dejanović**Vote:** 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1387

Links
[1] https://www.yahoo.com/tech/apple-fixes-serious-bug-download-the-update-now-83649096404.html
[2] http://en.wikipedia.org/wiki/Man-in-the-middle_attack
[3] http://9to5mac.com/2014/04/10/apple-says-heartbleed-security-flaw-did-not-affect-its-software-or-services/