

Onemogućavanje protokola SSLv3 u mrežnim servisima

Željko Boroš | 17 prosinca, 2014

U člancima o [ranjivosti OpenSSL-a](#), poznatijim kao [POODLE](#), spominjali smo samo web kao metu napada. Ali, svi znamo da se OpenSSL rabi i na dosta drugih servisa. U ovom trenutku kada se protokol SSLv3 pokazao kao nedorastao zadatku, ne bi bilo loše isključiti ga iz svih servisa koje rabite. Pokazat ćemo vam kako detektirati rabi li se SSLv3 na pojedinom servisu, te kako ga isključiti. Pa, krenimo redom.

Prvo, provjerimo postoji li uopće SSL (i koje točno inačice) na odabranom servisu (u ovom slučaju smo testirali **imaps**, iako je moguće na ovaj način testirati sve servise s podrškom za SSL/TLS):

Ispis smo znatno skratili, jer nas samo zanima vrti li se SSLv3. U ovom slučaju vidimo da on postoji. Nakon što smo ugasili SSLv3, ispis će biti ovakav:

Protokol SSLv3 se više ne može vidjeti, dakle uspješno smo ga onemogućili.

Postoji i drugi način provjere, preko naredbe **openssl**. Naredbu ćemo pokrenuti na ovaj način:

Ključne riječi koje tražimo su "**handshake failure**", što znači da servis ne podržava SSLv3.

Iako servisa ima mnogo, ograničili smo se na one koji se standardno vrte na CARNetovim poslužiteljima. Nakon svake izmjene, ne zaboravite restartati taj servis. Ukoliko se neki od korisnika buni da se odjednom "ne može spojiti", "ne radi mu" i slično, provjerite može li se njegov klijent nadograditi (štogod to bilo, browser, mail klijent ili drugo). Ukoliko se klijent ne može nadograditi, morat ćete vratiti postavke na staro dok taj problem ne riješite.

Apache

Datoteka: /etc/apache2/mods-enabled/ssl.conf

Postfix

Datoteka: /etc/postfix/main.cf

Dovecot

Datoteka: /etc/dovecot/conf.d/10-ssl.conf (ili bolje u svoju, primjerice 99-local.conf)

Vsftpd

Datoteka: /etc/vsftpd.conf

(samo ako je omogućen ssl_enable)

Proftpd

Datoteka: /etc/proftpd.conf

Slapd

SSL/TLS nije omogućen u standardnoj konfiguraciji kakva se rabi na CARNetovim poslužiteljima.