Nova ranjivost: POODLE 2

[1]Nakon što se u listopadu ove godine pojavila ranjivost POODLE [2], sad se pojavila nova ranjivost, nazvana POODLE 2, koja iskorištava slične mehanizme kao i originalna ranjivost. U ovom slučaju nije dovoljno samo onemogućiti SSLv3 protokol kako bi se izbjegla ranjivost, jer se u TLS-u nalaze srodne funkcije kao i u SSLv3. Tako je ovu ranjivost moguće pronaći u svim inačicama TLS-a (1.0, 1.1 i 1.2)!

Drugim riječima, iako se vodi borba na obje strane (klijentskoj i poslužiteljskoj), uskoro ćemo moći vidjeti POODLE 3 i kojekakve druge zanimljive nazive za ove propuste. Što možemo učiniti? Prvo, onemogućite SSLv3 u potpunosti. Ovo ćete napraviti tako da u datoteci **/etc/apache2/mods-enabled/ssl.conf** dodate sljedeće (odnosno prepravite postojeći redak):

```
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!RC4
```

Čestitamo, upravo ste imuni na POODLE (no ne u potpunosti na ovu ili neke kasnije inačice koje će se pojaviti). Doduše, sada se na vaše web-sjedište preko SSL/TLS-a ne mogu spojiti IE6 na WinXP (!), a vjerojatno i još poneki stariji Android.

Što se klijentske strane tiče, u Mozilla Firefoxu 34 je u potpunosti izbačen protokol SSLv3, a u inačici 40 će to napraviti i Chrome. Isto to će napraviti i drugi preglednici, ako već nisu.

Ukoliko želite testirati stanje vašeg poslužitelja "prije" i "poslije", postoji *on-line* provjera na adresi https://www.ssllabs.com/ssltest/index.html [3]. Nemojte očekivati ocjenu veću od "B".

Za tehničke detalje, pogledajte stranicu https://www.imperialviolet.org/2014/12/08/poodleagain.html [4] i https://community.qualys.com/blogs/securitylabs/2014/12/08/poodle-bites-tls [5].

Ukoliko želite svoje web-sjedište dodatno ojačati, možete pogledati preporuke na stranici https://testbit.eu/apache-sslciphersuite-without-poodle/ [6].

čet, 2014-12-11 13:56 - Željko Borš**Vijesti:** Sigurnosni propusti [7]
Sigurnost [8]
Kategorije: Servisi [9]
Vote: 5

Vaša ocjena: Nema Average: 5 (3 votes)

Source URL: https://sysportal.carnet.hr/node/1477

Links
[1] https://sysportal.carnet.hr/
[2] https://sysportal.carnet.hr/node/1446
[3] https://www.ssllabs.com/ssltest/index.html
[4] https://www.imperialviolet.org/2014/12/08/poodleagain.html
[5] https://community.qualys.com/blogs/securitylabs/2014/12/08/poodle-bites-tls
[6] https://testbit.eu/apache-sslciphersuite-without-poodle/
[7] https://sysportal.carnet.hr/taxonomy/term/14
[8] https://sysportal.carnet.hr/taxonomy/term/13
[9] https://sysportal.carnet.hr/taxonomy/term/28