Onemogućavanje protokola SSLv3 u mrežnim servisima

U člancima o ranjivosti OpenSSL-a [1], poznatijim kao POODLE [2], 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):

```
$ nmap -Pn -p T:imaps --script ssl-enum-ciphers localhost
PORT    STATE SERVICE
993/tcp open  imaps
| ssl-enum-ciphers:
|   SSLv3
|     Ciphers (10)
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - unknown strength
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
...
|   TLSv1.0
|     Ciphers (10)
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - unknown strength
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
...
|   TLSv1.1
|     Ciphers (10)
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - unknown strength
...
|   TLSv1.2
|     Ciphers (18)
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - unknown strength
...
|_  Least strength = unknown strength
```

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:

```
PORT    STATE SERVICE
993/tcp open  imaps
| ssl-enum-ciphers:
|   TLSv1.0
|     Ciphers (10)
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA - unknown strength
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA - strong
```

```
...
```

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:

```
$ openssl s_client -connect localhost:imaps -ssl3
CONNECTED(00000003)
3074578584:error:14094410:SSL routines:SSL3_READ_BYTES:
   sslv3 alert handshake failure:s3_pkt.c:1258:SSL alert number 40
3074578584:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:
   ssl handshake failure:s3_pkt.c:596:
```

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

```
SSLProtocol all -SSLv2 -SSLv3
```

Postfix

Datoteka: /etc/postfix/main.cf

```
# vrijedi samo ako je postavljen smtp_tls_security_level = mandatory
smtpd_tls_mandatory_protocols=!SSLv2,!SSLv3
```

Dovecot

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

```
ssl_protocols = !SSLv2 !SSLv3
```

Vsftpd

Datoteka: /etc/vsftpd.conf

(samo ako je omogućen ssl_enable)

```
ssl_sslv2 = no
ssl_sslv3 = no
ssl_tlsv1 = yes
```

Proftpd

Datoteka: /etc/proftpd.conf

```
TLSProtocol TLSv1
TlsCipherList HIGH:MEDIUM:+TLSv1:!SSLv2:!SSLv3
```

Slapd

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

sri, 2014-12-17 16:47 - Željko Borš**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1479

Links
[1] https://sysportal.carnet.hr/node/1477
[2] https://sysportal.carnet.hr/node/1446
[3] https://sysportal.carnet.hr/taxonomy/term/17
[4] https://sysportal.carnet.hr/taxonomy/term/28