Ozbiljan propust OpenSSL-a 1.0.1 i 1.0.2

Koriste li vaši poslužitelji OpenSSL verzije 1.0.1 ili 1.0.2, trebate odmah napraviti *roll-back* na stariju verziju (privremeni, jer starijim verzijama krajem 2015. godine prestaje podrška) ili instalirati najnoviji patch za verziju koju već koristite, upozorio je OpenSSL.org [1].

Riječ je o vrlo ozbiljnom propustu u verifikaciji certifikata u nizu, gdje zbog pogreške u algoritmu postoji mogućnost "preskakanja" sigurnosnih provjera u certifikatu, što otvara mogućnost lažne identifikacije certifikata kao autoritativnog za ulogu koja mu nije namijenjena. Kao najdrastičniji slučaj spominje se mogućnost zloupotrebe *leaf* certifikata (tj. zadnjeg u nizu certifikata koji počinje sa root CA certifikatom i završava sa *leaf* certifikatom) kao CA certifikata i izdavanje lažnih certifikata koji pokazuju na *leaf* certifikat kao svoj CA.

Lažnim predstavljanjem *leaf* certifikata kao *root CA* certifikata, MITM napadač može u komunikacijski kanal ubaciti lažne certifikate,
nakon čega presretanje i dešifriranje komunikacije postaje relativno trivijalno, pa čak i izmjena komuniciranih podataka "u letu" (noćna mora svakog developera telebanking aplikacije).

Ranjivi poslužitelj uspostavit će komunikacijski kanal kao da se ništa nije dogodilo, a ranjivi klijent neće ni na koji način biti obavješten o
sumnjivom certifikatu (osim ako se korisnik baš ne sjeti sam pregledati lanac certifikata i ima dovoljno znanja da prepozna lažirani lanac).

Iako je sigurnosni propust uistinu ozbiljne naravi, ako jedna od komponenti (poslužitelj ili klijent) ne koristi ranjivu verziju OpenSSL-a ranjivost nije moguće iskoristiti. Praktično, svi moderni *browseri* nisu osjetljivi na ovaj napad jer ne koriste OpenSSL. S druge strane, *embedded* uređaji i potencijalno veliki broj aplikacija koje u svom kodu sadrže OpenSSL kod mogli bi biti osjetljivi na napad koriste li ranjivu verziju protokola. Srećom, ranjivost postoji tek od verzija 1.0.1n i 1.0.2b koje su stare tek mjesec dana, što smanjuje vremenski period u kojem je proizvođač uređaja ili aplikacije mogao u svoj proizvod integrirati ove ranjive verzije protokola.

Ovo je primjer kako dobra praksa redovitog instaliranja sigurnosnih zakrpa u rijetkim slučajevima može biti lijek gori od bolesti: administratori koji svoje OpenSSL poslužitelje ne ažuriraju redovito nisu u opasnosti od ove ranjivosti, ali jesu od svih ranijih, dok su administratori koji savjesno obavljaju svoj posao nehotice otvorili bokove potencijalno vrlo opasnom i relativno lako iskoristivom sigurnosnom propustu.

Riječ je o vrlo nezgodnoj ranjivosti koja je, srećom, ograničena na uske scenarije. Stoga pokrpajte vaše poslužitelje bez previše panike (ali odmah), sjednite na pivo/kavu/čaj/sok/jednu_ljutu i otpišite ovu epizodukao uspješno riješen kuriozitet: i vaš je mali certifikat kratko vrijeme mogao glumiti da je CA.

Za programerski nastrojene čitateljie, evo dvije linije čija promjena "spaspava svijet":

```
xtmp = sk_X509_pop(ctx->chain);
X509_free(xtmp);
num--;
- ctx->last_untrusted--;
}
+ ctx->last_untrusted = sk_X509_num(ctx->chain);
```

```
retry = 1;
break;
}
```

https://github.com/openssl/openssl/commit/2aacec8f4a5ba1b365620a7b17fcce311ada93ad

sub, 2015-07-11 17:13 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1559

Links
[1] https://www.openssl.org/news/secadv_20150709.txt
[2] https://sysportal.carnet.hr/taxonomy/term/13