GnuTLS: a smijali smo se Appleu...

Nedavno objavljen članak [1] informirao nas je o nezgrapnom propustu u Appleovom kodu za provjeru digitalnih certifikata, zbog čega je neispravan certifikat mogao biti prihvaćen kao ispravan. Analizirali smo programski kod, smijali se korištenju "goto" naredbe i zaključili kako je, eto, i velika informatička tvrtka sposobna učiniti poprilično glupost. U međuvremenu dogodila se repriza u GnuTLS biblioteci.

U trenutku dok čitate ovaj tekst, vaši sustavi vjerojatno su već instalirali update biblioteke i računala vam više nisu izložena opasnosti vrlo sličnoj onoj u kojoj su bila Apple-ova računala. Naime, GnuTLS je baš poput iOS-a u nekim situacijama zbog pogrešno napisanog koda prihvaćao neispravne certifikate kao ispravne.

A da ironija bude veća, ovo je dio diff-a koda:

```
--- a/lib/x509/verify.c
+++ b/lib/x509/verify.c
@@ -141,7 +141,7 @@
if (result < 0)
{
gnutls_assert ();
- goto cleanup;
+ goto fail;
}
```

Sve izmjene na kodu lijepo možete vidjeti na Gitorius [2] stranici, uredno formatizirane i lijepo obojane.

Ponajprije, valja nam uočiti istu programersku nekvalitetu kakvu je demonstrirao Apple, oslanjajući se na "goto" naredbe, za koje vrijedi pravilo da ih treba izbjegavati poput priloga u e-mail porukama koje obećavaju brzu i laku zaradu na Internetu ili besplatan pristup porno stranicama - u svim slučajevima osim onda kada ih je vrlo nepraktično ili nemoguće izbjeći.

Razlog je jasan: goto naredbe razbijaju strukturiranost koda i lako mogu dovesti do pogrešaka koje se neće otkriti prilikom prevođenja programa, već prilikom korištenja aplikacije.

Problem sa GnuTLS kodom nije se krio direktno u goto naredbama, već u malo kompliciranijoj pogrešci: neke funkcije su vraćale brojčane vrijednosti, dok su druge funkcije očekivale Boolean vrijednosti, pa je svaki put kada bi funkcija vratila neku vrijednost različitu od nule, funkcija koja očekuje Boolean zaključila bi kako je ulaz "True". Specifičnost je ove pogreške što neće prihvatiti bilo kakav certifikat kao ispravan kao u slučaju iOS-a, ali se moguće posebno oblikovanim certifikatom "provući" kroz provjeru.

iOS i GnuTLS upravo fantastično demonstriraju kako bezazlena igra *goto* naredbama (plus ozbiljan nedostatak kontrole kvalitete koda) može rezultirati katastrofalnim posljedicama, jer kao i u slučaju iOS-a, naime, i GnuTLS ovu grešku vuče dugo [3], duže od deset godina – u oba slučaja, krucijalni sigurnosni problemi godinama nisu rješavani.

Da bi stvar bila zanimljivija, čini se kako je čovjek koji stoji iza otkrića pogreške isti čovjek koji je pogrešku [3] i napravio!

Ako vas je ova priča malo uplašila, ne trebate se bojati. Naime, pogreška je već patchirana i ako održavate serversku higijenu i redovito instalirate sigurnosne zakrpe, vaši su strojevi već nekoliko dana sigurni.

No, obzirom da postoje embedded uređaji i slične manje spravice čiji proizvođači nemaju običaj pratiti sigurnosne zakrpe i omogućavati uređajima da se preko Interneta "osvježe", ovaj sigurnosni problem mogli bismo susretati još godinama – posebice kod onih specijaliziranih uređaja kojima je potrebno promjeniti cijeli *firmware*, a proizvođač nema namjeru pozabaviti se tim problemom ili još gore – ako proizvođač više ne postoji.

sri, 2014-03-12 22:00 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [4]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1366

Links
[1] https://sysportal.carnet.hr/node/1360
[2] https://www.gitorious.org/gnutls/gnutls/commit/6aa26f78150ccbdf0aec1878a41c17c41d358a3b
[3] https://www.gitorious.org/gnutls/gnutls/commit/0fba2d908da6d0df821991ea5fdbeeda0f4ff089#lib/x509/verify.c
[4] https://sysportal.carnet.hr/taxonomy/term/14