Apple: goto fail

 Tipične računalne pogreške nastaju kodiranjem u brzini i uz nedovoljno pažnje. Srećom, mnoge od tih pogrešaka bivaju otkrivene već prilikom kompajliranja, kada kompajler prijavi grešku ili upozorenje. One koje se provuku prolaze kroz dugotrajnu proceduru provjere kvalitete i većinom bivaju ispravljene prije puštanja proizvoda na tržište. Taj proces nije idealan, no ovo što se dogodilo tvrtki Apple poprilično je nezgodan i zaista opasan problem.

Apple je nedavno u tišini izdao zakrpe za iOS i odbio ih detaljnije komentirati. Tako je samo zaintrigirao stručnjake za sigurnost koji su istražili problem i otkrili opasan propust u kodu koji verificira ispravnost SSL certifikata, a koji se nalazi u Appleovom kodu kojim je zamjenjen stari kod iz OS X 10.7 i starijih.

Ovo je izvorni kod problematičnog mjesta:

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
uint8_t *signature, UInt16 signatureLen)
{
OSStatus err;
...
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
goto fail;
goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
goto fail;
...
fail:
SSLFreeBuffer(&signedHashes);
SSLFreeBuffer(&hashCtx);
return err;
}
```

Vjerojatno vam je, ovako ponuđen na pladnju, problem odmah iskočio pred oči: programer je dva puta za redom napisao "goto fail;".

Na sumnju da je riječ o nedovoljno iskusnom programeru dovodi nas činjenica da je koristio naredbu za "pacere" ***goto*** kojoj programeri pribjegavaju tek onda kada logiku ne mogu zadati "normalnijim" grananjima, a želja za izbjegavanjem vitičastih zagrada za označavanje bloka naredbi, koja bi ovaj *copy&paste* problem eliminirala, dovela je do situacije u kojoj se naredba viška bespogovorno izvršava jer nije dio niti jednog uvjeta i tako faktički zaobilazi kontrolu SSL certifikata.

Krajnji rezultat je opasan sigurnosni propust u kojem svatko može podvaliti bilo kakav lažni SSL certifikat, a računalo/telefon će ga "progutati", otvorivši tako široku cestu malicioznim namjerama nepoznatih osoba.

Rješenje problema je što brži update OS-a na telefonima i uskoro na računalima [1], a u međuvremenu je moguće malo pomoći izbjegavanjem korištenja Safari browsera (ali istu rutinu

koriste i drugi [2] Appleovi proizvodi, odnosno korištenjem Open Source rješenja (Firefox, Thunderbird...) za komunikaciju s vanjskim svijetom.

Detalje o problemu ima Sophos [3], a na blogu ImperialViolet [4] pronaći ćete detalje o softverskom propustu.

uto, 2014-02-25 18:39 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1360

Links
[1] http://appleinsider.com/articles/14/02/24/apple-nearing-release-of-os-x-1092-with-support-for-facetime-audio-fixes-for-mail-safari
[2] https://twitter.com/ashk4n/status/437650438079672320/photo/1
[3] http://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/
[4] https://www.imperialviolet.org/2014/02/22/applebug.html
[5] https://sysportal.carnet.hr/taxonomy/term/14